![CISCO]

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

First Published: 2020-08-10

Last Modified: 2024-07-24

CONTENTS

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

iii

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

iv

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

v

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

vi

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

vii

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

viii

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

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

ix

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

x

High-Availability Seamless Redundancy (HSR)

Information About HSR

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

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

Note HSR is supported on IE3400 Rugged and IE3400 Heavy Duty Series Switches (see Guidelines and Limitations, on page 21 for supported SKUs). The term *switch* in this document refers to the IE3400 Rugged and IE3400 Heavy Duty Series Switches unless otherwise noted.

The switch supports two HSR modes of operation: HSR-SAN and HSR-PRP. HSR-PRP mode is added in the Cisco IOS XE 17.14.1 release. The switch can support only one mode at a time. When operating in HSR-SAN mode, no PRP instances can be created. When operating in HSR-PRP mode, a single PRP interface is identified in addition to the two HSR ring port interfaces. This is different than creating a PRP instance

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

1

which has a full PRP channel port with two interfaces on same switch. When operating in HSR-PRP mode, it is expected that two HSR ring nodes will have PRP interfaces, a PRP interface for LAN A and B.

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

The following figure shows an example of an HSR ring as described in IEC 62439-3. In this example, the RedBox is an IE 3400.

Figure 1: Example of HSR Ring Carrying Unicast Traffic
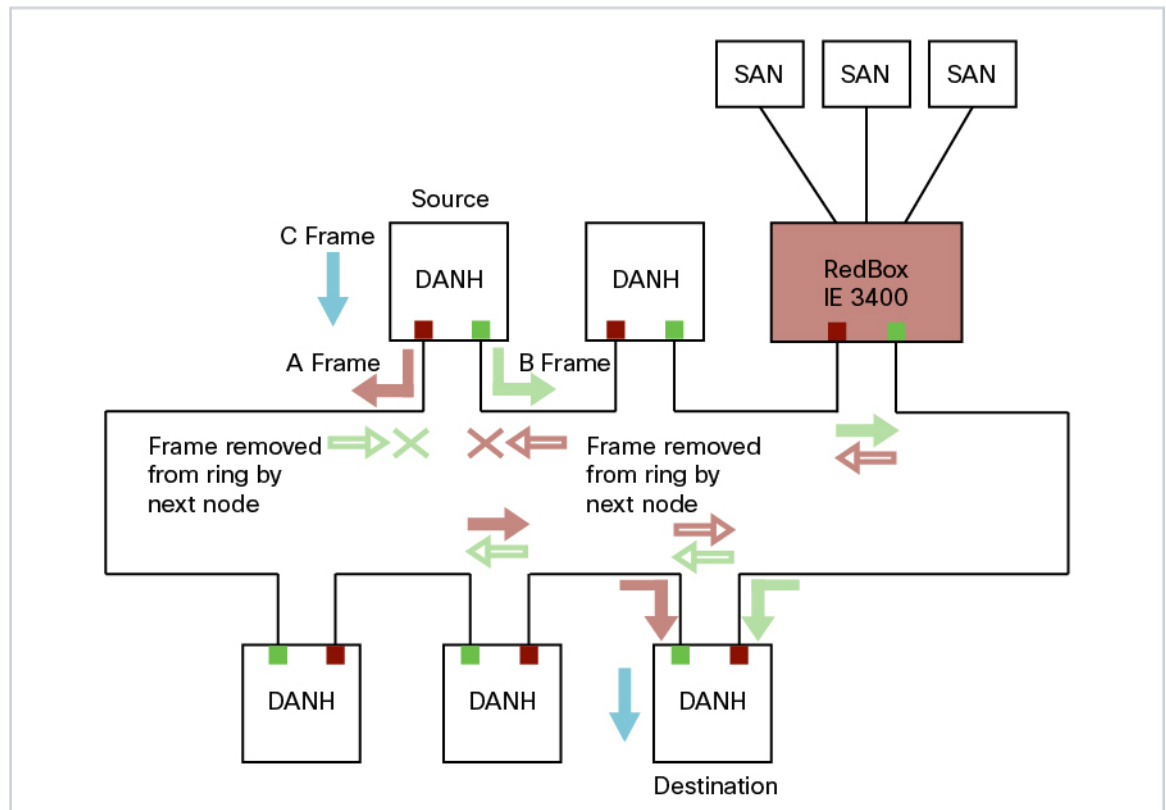
Devices that do not support HSR out of the box (for example, laptops and printers) cannot be attached to the HSR ring directly because all HSR capable devices must be able to process the HSR header on packets received from the ring and add the HSR header to all packets sent into the ring. These nodes are attached to the HSR ring through a RedBox. As shown in the figure above, the RedBox has two ports on the DANH side. Non-HSR SAN devices are attached to the upstream switch ports. The RedBox generates the supervision frames on behalf of these devices so that they are seen as DANH devices on the ring. Because the RedBox emulates these as DANH, they are called Virtual Doubly Attached Nodes (VDAN).

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

2

Loop Avoidance

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

- Unicast packet with destination inside the ring: When the unicast packet reaches the destination node, the packet is consumed by the respective node and is not forwarded.

- Unicast packet with destination not inside the ring: Because this packet does not have a destination node in the ring, it is forwarded by every node in the ring until it reaches the originating node. Because every node has a record of the packet it sent, along with the direction in which it was sent, the originating node detects that packet has completed the loop and drops the packet.

- Multicast packet: A multicast packet is forwarded by each node because there can be more than one consumer of this packet. For this reason a multicast packet always reaches the originating node. However, every node will check whether it has already forwarded the received packet through its outgoing interface. Once the packet reaches the originating node, the originating node determines that it already forwarded this packet and drops the packet instead of forwarding it again.

HSR RedBox Modes of Operation

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

HSR-SAN Mode

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

- A source DANH sends a frame passed from its upper layers ("C" frame), prefixes it with an HSR tag to identify frame duplicates, and sends the frame over each port ("A" frame and "B" frame).

- A destination DANH receives two identical frames from each port within a certain interval. The destination DANH removes the HSR tag of the first frame before passing it to its upper layers and discards any duplicate.

- Each node in the HSR ring forwards frames received from one port to the other port of the HSR pair. A node will not forward frames received on one port to the other under the following conditions:

  - The received frame returns to the originating node in the ring.

  - The frame is a unicast frame with a destination MAC address of a node upstream of the receiving node.

  - The node had already sent the same frame in the same direction. This rule prevents a frame from spinning in the ring in an infinite loop.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

3

HSR-SAN Interfaces

HSR-SAN mode is supported on interfaces GigabitEthernet 1/1-4. HSR ring 1 is configured as a pair of ports: G1/1 and G1/2 or G1/3 and G1/4.

HSR-PRP (Dual RedBox Mode)

HSR-PRP mode, also called Dual RedBox mode, is used to bridge HSR and PRP networks. Dual RedBox mode is supported on IE3400 and IE3400H switches only.

In this mode, two different RedBoxes connect to LAN A and LAN B of the PRP network. Two ports connect to the HSR ring and one port connects to one of the two PRP LANs. The traffic on the upstream interlink port connecting the RedBox to the PRP network is PRP-tagged. In HSR-PRP mode, the RedBox extracts data from the PRP frame and generates the HSR frame using this data, and performs the reverse in the opposite direction. To avoid loops and use network bandwidth effectively, the RedBox does not transmit frames already transmitted in same direction (see Loop Avoidance, on page 3).

The following figure shows an HSR ring connected to a PRP network through two RedBoxes, one for each LAN. In this example, the source frame originates in the PRP network. RedBoxes are configured to support PRP traffic on the interlink ports and HSR traffic on the ring ports. Nodes connected to the HSR-PRP Redbox act as a SAN to the PRP Redbox and a VDAN to the HSR-PRP Dual Redbox.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

4
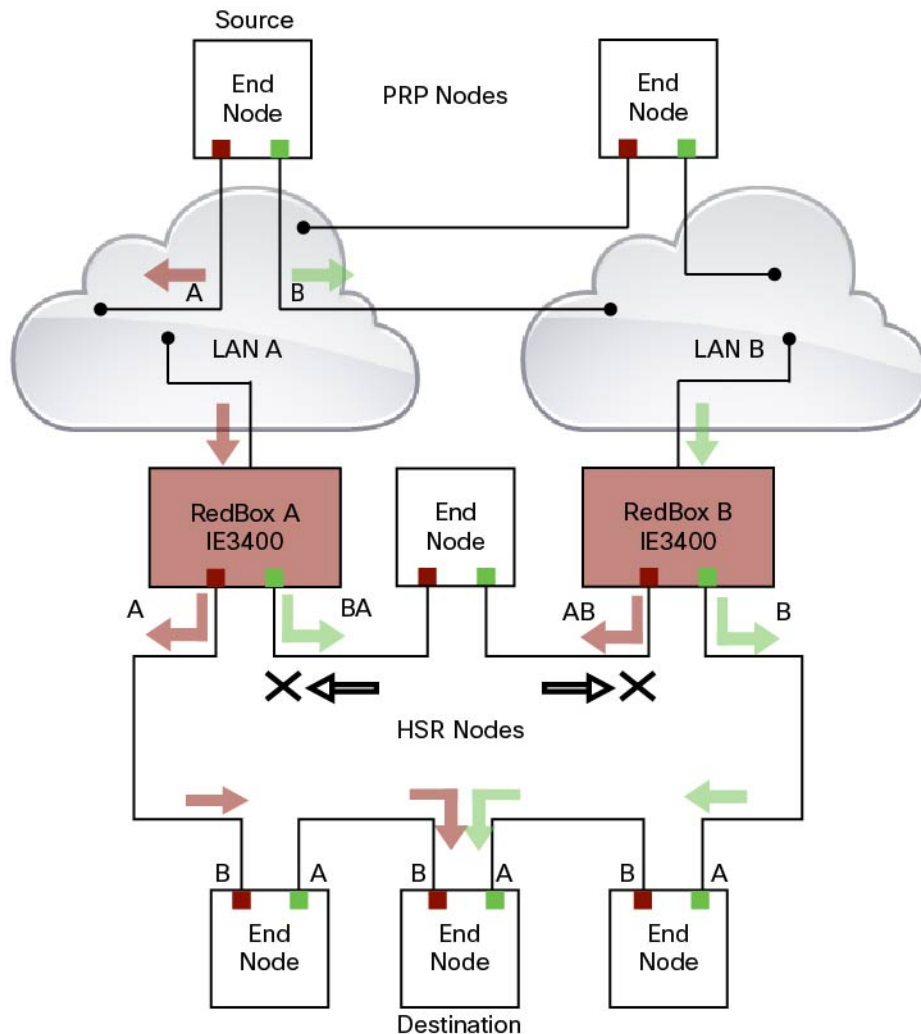
The sequence number from the PRP RCT is reused for the HSR tag and vice versa to allow frame identification from one redundancy network to the other and to identify the pairs and duplicates on either network. In the figure above, RedBox A and RedBox B send the same frame (A and AB and B and BA, respectively), but a RedBox does not transmit a frame that it already received.

Every DANH device generates its own sequence number, which is incremented for each outgoing frame. When a packet is switched from HSR to PRP or PRP to HSR, the sequence number is taken from the incoming packet so the same sequence number is used. Any node, whether it is an intermediate or final destination in the HSR or PRP network, uses the source MAC address and sequence number as the key for duplicate packet detection. Because the source address is expected to be unique for each node, there are no overlapping sequence numbers between different nodes.

Multicast frames or unicast frames without a receiver in the ring (arrows with the black outline in the figure) are removed by the RedBox that inserted them into the ring, if they originated from outside the ring. For this purpose, the frames carry a LAN identifier that is also the RedBox identifier.

The following figure shows an HSR ring coupled to a PRP network, where the source frame originates in the HSR ring.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches ■

5
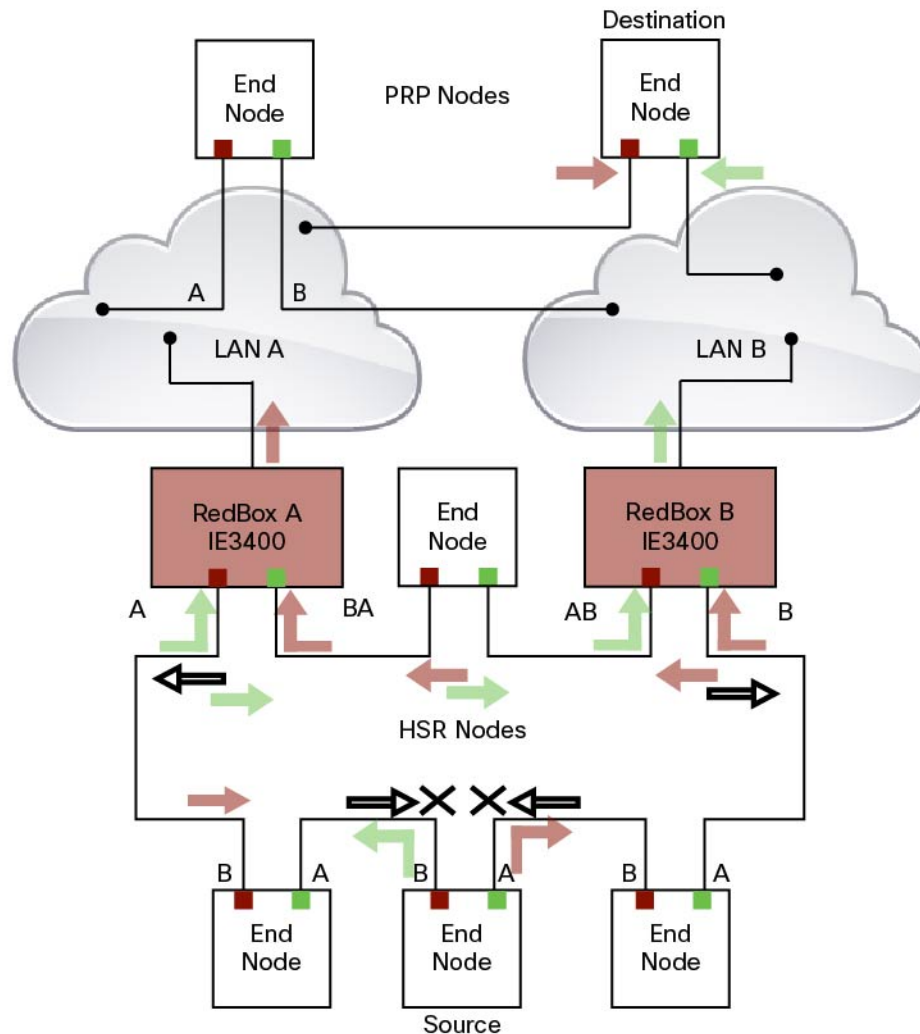
To prevent frames from being reinjected into the PRP network through the other RedBox, each HSR frame carries the 4-bit PathId, which identifies the PRP network from which the frame came originally. RedBoxes are configured and identified by the PathId of the PRP LAN to which they are attached.

Different PathIds can be used to bridge more than one PRP network to an HSR ring. Likewise, more than one HSR ring can be bridged to a PRP network.

PRP is not needed for HSR-PRP to function in the IE3400. Any third port can be connected to PRP LAN A or LAN B network without PRP or any specific configurations.

PRP Supervision frames are sent toward PRP LAN A or LAN B from conversion of HSR Supervision Frames originated from DANHs and VDANs of HSR RedBoxes in the HSR ring. The HSR-PRP Redbox does not generate them but passes them along.

Packet flow in HSR-PRP

Packets coming from PRP network in the coupled PRP LAN-A or LAN-B are expected to have an RCT (Redundancy Control Trailer) tag. The switch removes the RCT and transfers the information to the HSR

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

6

header using the programmed Net ID and LAN ID, recalculates the CRC, and sends the modified packet out to both ring A and ring B. If the packets originate from a SAN in the coupled PRP network, the switch treats it similarly as a VDAN to the HSR ring.

Egress Data Path—Packets coming from a SAN or PRP LAN A or LAN B to the HSR ring:

- For PRP packets, the switch converts the PRP RCT to an HSR tag for all packets (transfers Sequence Number and LAN ID from PRP to HSR).

- For SAN packets, the switch just inserts the HSR tag as is done in HSR-SAN RedBox mode.

- The switch needs to learn the MAC source address and add it to the Proxy Node table (VDAN table) with a new additional bit that allows the switch to distinguish between DANP or SAN. This allows the ingress path to determine whether to include the RCT trailer or not.

Ingress Data Path—Packets coming from the HSR ring to a SAN or PRP LAN A or LAN B:

- If the Proxy Node table or VDAN table lookup of the MAC destination address returns DANP, the switch converts the HSR tag to PRP RCT for accepted packets (transfers Sequence Number and LAN ID from HSR to PRP RCT).

- If the Proxy Node table or VDAN table lookup of the MAC destination address returns SAN, the switch strips the HSR tag and sends the packet without the RCT.

HSR-PRP Interfaces

In HSR-PRP Dual RedBox mode, two ports are connected to the HSR ring, and one port is connected to the PRP LAN A or LAN B network. The two ports that connect to the HSR ring are fixed (Gi1/1 and Gi1/2). The port connected to PRP LAN A or LAN B can be any other port from the base module or expansion module. All remaining ports of the HSR-PRP RedBox (base module or expansion module ports) can be used for any other purpose, for example, to connect a DHCP server. These ports act as non-HSR/PRP nodes (SANs/VDANs) in the topology.

Connecting Multiple PRP Networks to an HSR Ring

A maximum of six PRP networks, identified by the PathId, can be connected to the same HSR ring. The 4-bit PathId consists of the following:

- The 3-bit NetId (1 to 6), which identifies a PRP network and the two RedBoxes that connect the PRP network to an HSR ring.

- The 1-bit LanId (LAN A = 0 and LAN B = 1)

NetId values are as follows:

- 0 for regular HSR frames

- 1 to 6 for frames originating from a PRP network

- 7 is reserved

The following table lists the combinations of NetIds and LanIds for Redbox-A and Redbox-B.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

7

PathId		
NetId	**LanId**	
	RedBox-A	**RedBox-B**
001	0	1
010	0	1
011	0	1
100	0	1
101	0	1
110	0	1
000	**Used for Local HSR Ring**	
111	**Reserved**	

The following figure shows an example of an HSR ring connected to two PRP networks.
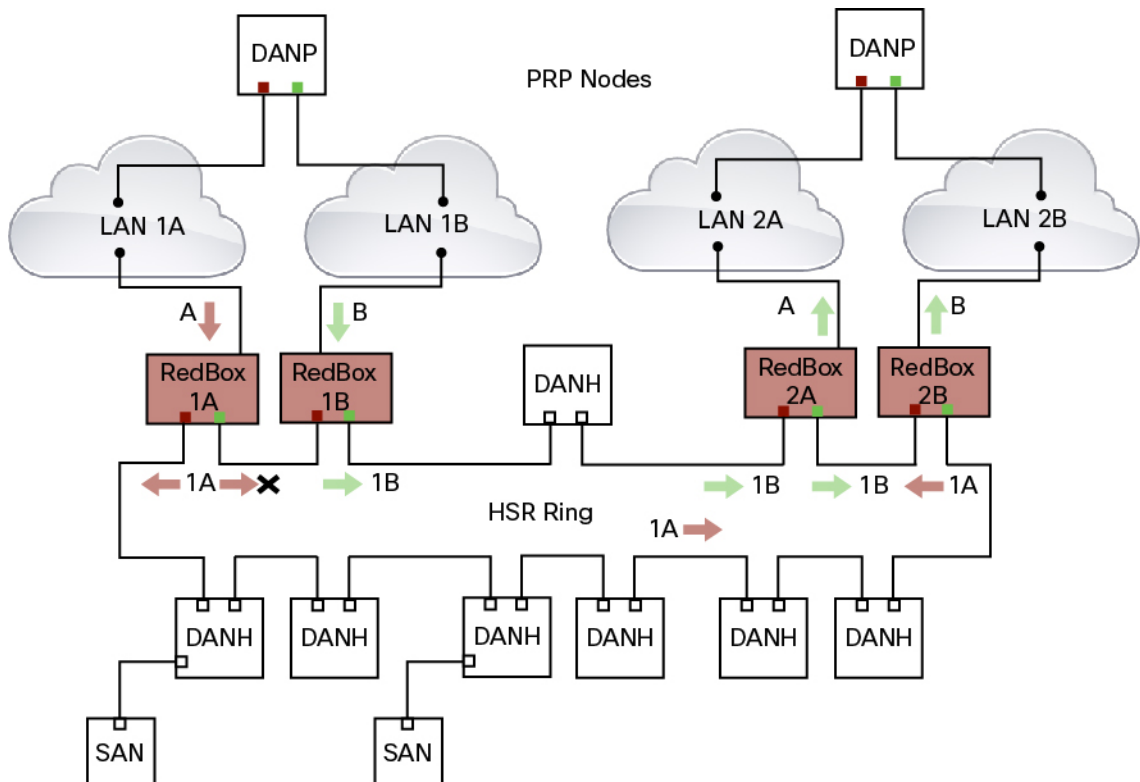
To prevent reinjection of frames coming from one PRP network into another PRP network or from the other LAN of the same PRP network, a RedBox only forwards frames that do not carry its own PathId from the HSR ring.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

8

When a PRP frame from LAN A or from LAN B of a PRP network with a given NetId is inserted to the HSR ring, a RedBox inserts its own NetId and the LanId "A" or "B" into the PathId of the HSR tag.

When forwarding a frame from the HSR ring to a PRP network, the RedBox inserts the LanId "A" or "B" into the RCT.

Connecting Multiple HSR Rings to a PRP Network

A PRP network can be connected to any number of HSR rings, but these rings cannot be connected to each other because this would create loops. The following figure shows an example of three HSR rings connected to one PRP LAN.
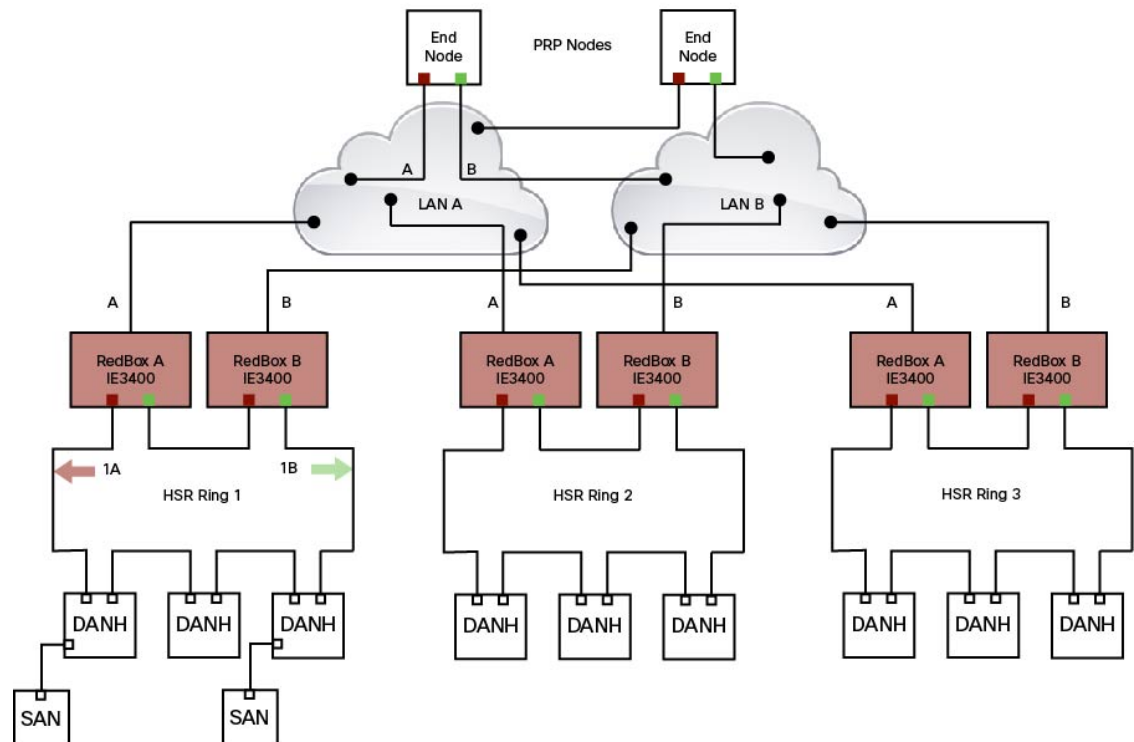
CDP and LLDP for HSR

HSR supports the Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP). CDP and LLDP are Layer 2 neighbor discovery protocols. Both CDP and LLDP can provide information about nodes directly connected to the device. They also provide additional information such as the local and remote interface and device names.

When CDP or LLDP is enabled, you can use the CDP or LLDP information to find the adjacent nodes on an HSR ring and their status. You can then use the neighbor information from each node to determine the complete HSR network topology and debug and locate ring faults.

CDP and LLDP are configured on physical interfaces only.

For more information, see Configuring an HSR Ring, on page 26 and Verifying Configuration, on page 29.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

9

PTP over HSR

Precision Time Protocol (PTP) is supported on the IE3400 Rugged and IE3400 Heavy Duty Series Switches for the PTP Power Profile only.

Because the PTP 1588 standard does not currently account for clocks synchronized over redundant, simultaneously active paths, HSR must handle PTP packets differently that other packet types. To provide high availability for PTP through redundancy, the HSR duplicate/discard logic is not used for PTP packets.

To understand how PTP clock syncronization works in an HSR network, suppose that a VDAN/SAN is the PTP grandmaster clock (GMC). Dually attached devices receive PTP synchronization information over both their HSR ports. However, only one of the ports (referred to as time recipient) is used to synchronize the local clock. The other HSR port (referred to as PASSIVE) continues to receive synchronization information, but is not used to synchronize the local clock. Suppose that RedBox 2 has its port-A as time recipient and port-B as PASSIVE. When port-A goes down, the port-B port takes over as the time recipient and is used to continue synchronizing the local clock on RedBox 2.

Note Cisco is moving from the traditional Master/Slave nomenclature. In this document, the terms *Grandmaster clock (GMC)* or *time source* and *time recipient* are used instead.

The PTP grandmaster in an HSR network can be a RedBox, a VDAN/SAN, or a DANH.

To use PTP over HSR, configure HSR and PTP separately. PTP over HSR works without any additional configuration. Note that in most cases, you do not need to perform any PTP configuration on the interfaces because PTP is enabled by default on all physical ethernet interfaces.

Supported PTP Profiles and Modes

PTP over HSR is supported only for the for the PTP Power Profile. For unsupported PTP profiles, PTP traffic flows over HSR port-A only.

The following table shows the HSR support for PTP profiles, clock modes and RedBox types.

PTP Profile	Clock Mode	Supported?	HSR Redbox Type as per IEC 62439-3
Power Profile	BC	Yes	HSR RedBox as doubly attached BC (DABC) with P2P
	P2P TC	Yes	HSR RedBox as doubly attached TC (DATC) with P2P
	GMC-BC	No	Not applicable
	Forward	No	Not applicable
Default Profile	BC	No	Not applicable
	E2E TC	No	Not applicable

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

10

HSR RedBox as Doubly Attached BC (DABC) with P2P

This section describes the operation of PTP over HSR using an example where RedBox M and RedBox S are configured to run in Power Profile as Boundary Clocks that use the Peer-to-Peer delay measurement mechanism.
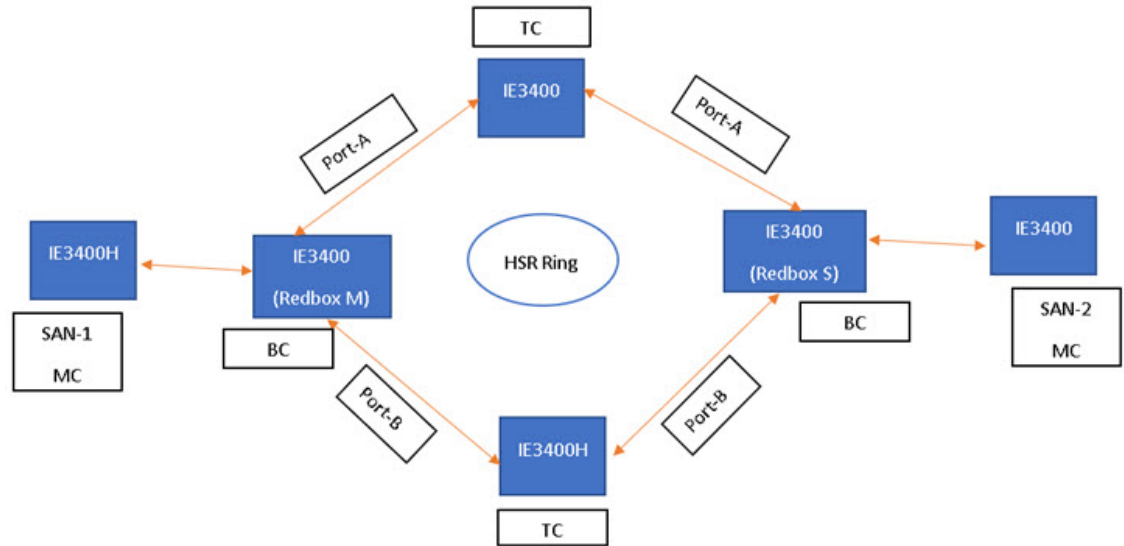
Assume for this example that SAN-1 is the GMC. All the clocks are configured to run Peer-to-Peer Delay measurement and the peer delay is regularly calculated and maintained on every link shown in the figure. The BMCA on RedBox M determines the port to SAN-1 to be connected to the time source. The PTP protocol running on RedBox M will forward Sync and Follow_up messages on ports A and B.

On RedBox S, the regular BMCA operation determines port A to be time recipient and port B to be PASSIVE. However, with the knowledge that ports A and B are part of the same HSR ring, port B is forced into PASSIVE_SLAVE state and port A becomes active for PTP.

Port A works as a regular time recipient port. It uses the Sync and Follow_Up messages along with their correction field to calculate the delay and offset from time source and synchronize the local clock. (Unlike an E2E BC, it does not need to generate Delay_Req messages since all the link delays and residence times along the PTP path are accumulated in the correction field of the Follow_Up messages.)

Port B, which is in PASSIVE_SLAVE state operates as follows: Just like port A, it maintains the delay and offset from time source, but does not perform any operation on the local clock. Having all the synchronization information available enables it to seamlessly take over as the new time recipient in case port A loses communication with the GMC. Note that on IE switch platforms we currently do not support PTP profile conversion. For example, if RedBox S in the figure above were an IE switch, it would not support the Delay_Req/Delay_Resp message exchange. It would only support the Peer-to-Peer delay measurement mechanism using PDelay messages.

Configuration Example

```
SAN-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SAN-1(config)#ptp profile power
SAN-1(config)#ptp mode boundary pdelay-req
SAN-1(config)#ptp priority1 1
SAN-1(config)#end

SAN-2#conf t
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

11

```
Enter configuration commands, one per line.  End with CNTL/Z.
SAN-2(config)#ptp profile power
SAN-2(config)#ptp mode boundary pdelay-req
SAN-2(config)#end

REDBOX-M#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
REDBOX-M(config)#ptp profile power
REDBOX-M(config)#ptp mode boundary pdelay-req
REDBOX-M(config)#end

REDBOX-S#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
REDBOX-S(config)#ptp profile power
REDBOX-S(config)#ptp mode boundary pdelay-req
REDBOX-S(config)#end

DANH-TOP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DANH-TOP(config)#ptp profile power
DANH-TOP(config)#ptp mode p2ptransparent
DANH-TOP(config)#end

DANH-BOTTOM#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DANH-BOTTOM(config)#ptp profile power
DANH-BOTTOM(config)#ptp mode p2ptransparent
DANH-BOTTOM(config)#end

SAN-1#sh ptp parent
 PTP PARENT PROPERTIES
  Parent Clock:
  Parent Clock Identity: 0x0:35:1A:FF:FE:94:4F:0
  Parent Port Number: 0
  Observed Parent Offset (log variance): N/A
  Observed Parent Clock Phase Change Rate: N/A

  Grandmaster Clock:
  Grandmaster Clock Identity: 0x0:35:1A:FF:FE:94:4F:0
  Grandmaster Clock Quality:
 Class: 248
 Accuracy: Unknown
 Offset (log variance): N/A
 Priority1: 1
 Priority2: 128

SAN-2#sh ptp parent
 PTP PARENT PROPERTIES
  Parent Clock:
  Parent Clock Identity: 0x0:29:C2:FF:FE:3C:6A:C0
  Parent Port Number: 9
  Observed Parent Offset (log variance): N/A
  Observed Parent Clock Phase Change Rate: N/A

  Grandmaster Clock:
  Grandmaster Clock Identity: 0x0:35:1A:FF:FE:94:4F:0
  Grandmaster Clock Quality:
 Class: 248
 Accuracy: Unknown
 Offset (log variance): N/A
 Priority1: 1
 Priority2: 128

REDBOX-M#sh ptp parent
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

12

```
 PTP PARENT PROPERTIES
  Parent Clock:
  Parent Clock Identity: 0x0:35:1A:FF:FE:94:4F:0
  Parent Port Number: 3
  Observed Parent Offset (log variance): N/A
  Observed Parent Clock Phase Change Rate: N/A

  Grandmaster Clock:
  Grandmaster Clock Identity: 0x0:35:1A:FF:FE:94:4F:0
  Grandmaster Clock Quality:
 Class: 248
 Accuracy: Unknown
 Offset (log variance): N/A
 Priority1: 1
 Priority2: 128

REDBOX-S#sh ptp parent
 PTP PARENT PROPERTIES
  Parent Clock:
  Parent Clock Identity: 0x0:29:C2:FF:FE:3C:5D:80
  Parent Port Number: 3
  Observed Parent Offset (log variance): N/A
  Observed Parent Clock Phase Change Rate: N/A

  Grandmaster Clock:
  Grandmaster Clock Identity: 0x0:35:1A:FF:FE:94:4F:0
  Grandmaster Clock Quality:
 Class: 248
 Accuracy: Unknown
 Offset (log variance): N/A
 Priority1: 1
 Priority2: 128

DANH-TOP#sh ptp parent
 PTP PARENT PROPERTIES
  Parent Clock:
  Parent Clock Identity: 0x0:29:C2:FF:FE:3C:5D:80
  Parent Port Number: 3
  Observed Parent Offset (log variance): N/A
  Observed Parent Clock Phase Change Rate: N/A

  Grandmaster Clock:
  Grandmaster Clock Identity: 0x0:35:1A:FF:FE:94:4F:0
  Grandmaster Clock Quality:
 Class: 248
 Accuracy: Unknown
 Offset (log variance): N/A
 Priority1: 1
 Priority2: 128

DANH-BOTTOM#sh ptp parent
 PTP PARENT PROPERTIES
  Parent Clock:
  Parent Clock Identity: 0x0:29:C2:FF:FE:3C:5D:80
  Parent Port Number: 4
  Observed Parent Offset (log variance): N/A
  Observed Parent Clock Phase Change Rate: N/A

  Grandmaster Clock:
  Grandmaster Clock Identity: 0x0:35:1A:FF:FE:94:4F:0
  Grandmaster Clock Quality:
 Class: 248
 Accuracy: Unknown
 Offset (log variance): N/A
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

13

```
        Priority1: 1
        Priority2: 128
```

HSR RedBox as Doubly Attached TC (DATC) with P2P

This section describes the operation of PTP over HSR using an example where RedBox M and RedBox S are configured to run in Power Profile as Transparent Clocks.
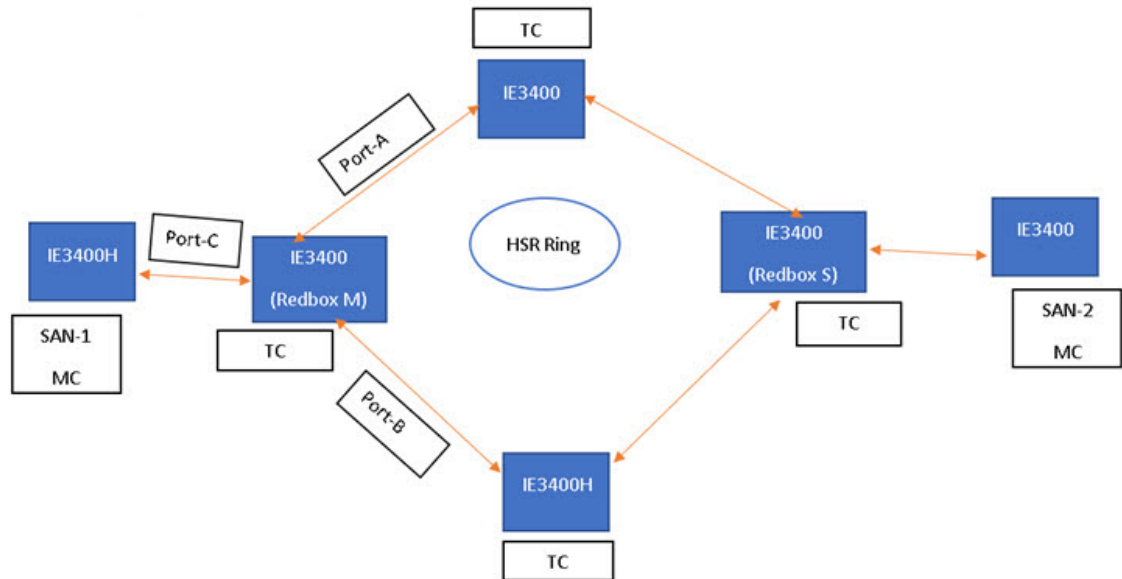
Assume for this example that SAN-1 is the GMC. All the clocks are configured to run Peer-to-Peer Delay measurement and the peer delay is regularly calculated and maintained on every link shown in the figure. RedBox M and RedBox S run BMCA even though it is not mandatory for a P2P TC to run BMCA. On RedBox M, the BMCA on redbox M determines the port to SAN-1 to be connected to the time source. RedBox M forwards all Sync and Follow_Up messages received on port C out of ports A and B.

On RedBox S, port A is determined to be time recipient and port B to be PASSIVE_SLAVE as described earlier.

Port A operates as follows: It uses the Sync and Follow_Up messages along with their correction field to calculate the delay and offset from time source and synchronize the local clock. (Unlike a E2E BC, it does not need to generate Delay_Req messages since all the link delays and residence times along the PTP path are accumulated in the correction field of the Follow_Up messages.) It also forwards the Sync and Follow_Up messages out of port C.

Port B operates as follows: Just like port A, it maintains the delay and offset from time source, but does not perform any operation on the local clock. Having all the synchronization information available enables it to seamlessly take over as the new time recipient in case port A loses communication with the GMC. Post-processing, it drops the Sync/Follow_Up messages since the copy of Sync/Follow_Up that arrives on port A is forwarded out of port C.

Configuration Example

```
SAN-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SAN-1(config)#ptp profile power
SAN-1(config)#ptp mode boundary pdelay-req
SAN-1(config)#ptp priority1 1
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

14

```
SAN-1(config)#end
SAN-2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SAN-2(config)#ptp profile power
SAN-2(config)#ptp mode boundary pdelay-req
SAN-2(config)#end
REDBOX-M#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
REDBOX-M(config)#ptp profile power
REDBOX-M(config)# ptp mode p2ptransparent
REDBOX-M(config)#end
REDBOX-S#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
REDBOX-S(config)#ptp profile power
REDBOX-S(config)# ptp mode p2ptransparent
REDBOX-S(config)#end
DANH-TOP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DANH-TOP(config)#ptp profile power
DANH-TOP(config)#ptp mode p2ptransparent
DANH-TOP(config)#end
DANH-BOTTOM#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DANH-BOTTOM(config)#ptp profile power
DANH-BOTTOM(config)#ptp mode p2ptransparent
DANH-BOTTOM(config)#end
SAN-1#sh ptp parent
 PTP PARENT PROPERTIES
  Parent Clock:
  Parent Clock Identity: 0x0:35:1A:FF:FE:94:4F:0
  Parent Port Number: 0
  Observed Parent Offset (log variance): N/A
  Observed Parent Clock Phase Change Rate: N/A

  Grandmaster Clock:
  Grandmaster Clock Identity: 0x0:35:1A:FF:FE:94:4F:0
  Grandmaster Clock Quality:
 Class: 248
 Accuracy: Unknown
 Offset (log variance): N/A
 Priority1: 1
 Priority2: 128
SAN-2#sh ptp parent
 PTP PARENT PROPERTIES
  Parent Clock:
  Parent Clock Identity: 0x0:35:1A:FF:FE:94:4F:0
  Parent Port Number: 3
  Observed Parent Offset (log variance): N/A
  Observed Parent Clock Phase Change Rate: N/A

  Grandmaster Clock:
  Grandmaster Clock Identity: 0x0:35:1A:FF:FE:94:4F:0
  Grandmaster Clock Quality:
 Class: 248
 Accuracy: Unknown
 Offset (log variance): N/A
 Priority1: 1
 Priority2: 128
REDBOX-M#sh ptp parent
 PTP PARENT PROPERTIES
  Parent Clock:
  Parent Clock Identity: 0x0:35:1A:FF:FE:94:4F:0
  Parent Port Number: 3
  Observed Parent Offset (log variance): N/A
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

15

```
                Observed Parent Clock Phase Change Rate: N/A

                Grandmaster Clock:
                Grandmaster Clock Identity: 0x0:35:1A:FF:FE:94:4F:0
                Grandmaster Clock Quality:
               Class: 248
               Accuracy: Unknown
               Offset (log variance): N/A
               Priority1: 1
               Priority2: 128
            REDBOX-S#sh ptp parent
             PTP PARENT PROPERTIES
                Parent Clock:
                Parent Clock Identity: 0x0:35:1A:FF:FE:94:4F:0
                Parent Port Number: 3
                Observed Parent Offset (log variance): N/A
                Observed Parent Clock Phase Change Rate: N/A

                Grandmaster Clock:
                Grandmaster Clock Identity: 0x0:35:1A:FF:FE:94:4F:0
                Grandmaster Clock Quality:
               Class: 248
               Accuracy: Unknown
               Offset (log variance): N/A
               Priority1: 1
               Priority2: 128
            DANH-TOP#sh ptp parent
             PTP PARENT PROPERTIES
                Parent Clock:
                Parent Clock Identity: 0x0:35:1A:FF:FE:94:4F:0
                Parent Port Number: 3
                Observed Parent Offset (log variance): N/A
                Observed Parent Clock Phase Change Rate: N/A

                Grandmaster Clock:
                Grandmaster Clock Identity: 0x0:35:1A:FF:FE:94:4F:0
                Grandmaster Clock Quality:
               Class: 248
               Accuracy: Unknown
               Offset (log variance): N/A
               Priority1: 1
               Priority2: 128
            DANH-BOTTOM#sh ptp parent
             PTP PARENT PROPERTIES
                Parent Clock:
                Parent Clock Identity: 0x0:35:1A:FF:FE:94:4F:0
                Parent Port Number: 3
                Observed Parent Offset (log variance): N/A
                Observed Parent Clock Phase Change Rate: N/A

                Grandmaster Clock:
                Grandmaster Clock Identity: 0x0:35:1A:FF:FE:94:4F:0
                Grandmaster Clock Quality:
               Class: 248
               Accuracy: Unknown
               Offset (log variance): N/A
               Priority1: 1
               Priority2: 128
```

HSR Alarms

An HSR ring can generate the following two alarms:

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

16

• Partial Ring Fault: This fault is generated by an HSR RedBox when one of its physical ring ports/links is down. Because the packets can be sent using the redundant path, this is considered as a partial fault. However, this fault still requires user intervention to restore the ring. This is a minor fault and cannot be associated with an external hardware alarm relay.

• Full Ring Fault: This fault is generated by an HSR RedBox when both of its physical ring ports/links are down. This is a catastrophic failure and needs immediate attention. This is a major fault and can be associated with an external hardware alarm relay.

When an event that raises an alarm is generated, it can be associated with one or more of the following actions to notify the user:

• Syslog: A syslog is generated when the Alarm is raised/cleared.

• SNMP Notification: SNMP notification is sent when the alarm is raised/cleared.

• Relay output: External relay contacts can be asserted/de-asserted in response to the alarm. Relays are activated by major faults only.

See for steps to configure HSR alarms.

The following table lists the HSR events and their representations.

Event Number	Event Description	System Log (Level)	Alert/Alarm Log	Alarm LED and Output relay
1	Ring goes from UP to DOWN state.	2	2	Major Alarm/Assert
2	Ring goes from DOWN to UP state.	6	6	De-assert
3	One ring port goes DOWN, the other ring port and the ring itself is UP.	3	3	
4	Both ring ports are UP again.	6	6	

You can view currently active alarms using the **show facility alarm status** command. The following example shows alarm status for minor and major HSR alarms:

```
Switch#show facility-alarm status
Source          Severity    Description                     Relay   Time
Switch           MINOR     34 HSR ring is partially down       MAJ    Oct 24 2017 10:16:10

-------
Switch# show facility-alarm status
Source          Severity    Description                     Relay    Time
Switch           MAJOR     33 HSR ring is down                 MAJ     Oct 24 2017 10:17:07
```

The following examples show the syslog entries that are generated for each HSR alarm event assertion and clear event (if configured):

• Syslog generated on occurrence of Partial fault:

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

17

```
Oct 24 11:07:13.952 IST: %HSR_ALARM-3-HSR_PARTIALFAULT: The HSR ring in now in PARTIAL
 FAULT state
```

- Syslog generated when the Partial fault is cleared:

```
Oct 24 11:07:38.032 IST: %HSR_ALARM-3-HSR_PARTIALFAULT: The HSR ring in now in PARTIAL
 FAULT state - event cleared
```

- Syslog generated on occurrence of Full fault:

```
Oct 24 11:07:38.036 IST: %HSR_ALARM-2-HSR_RINGFAULT: The HSR ring in now in FAULT state
```

- Syslog generated when the Full fault is cleared:

```
Oct 24 11:08:19.082 IST: %HSR_ALARM-2-HSR_RINGFAULT: The HSR ring in now in FAULT state
 - event cleared
```

HSR Uplink Redundancy Enhancement

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

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

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

18
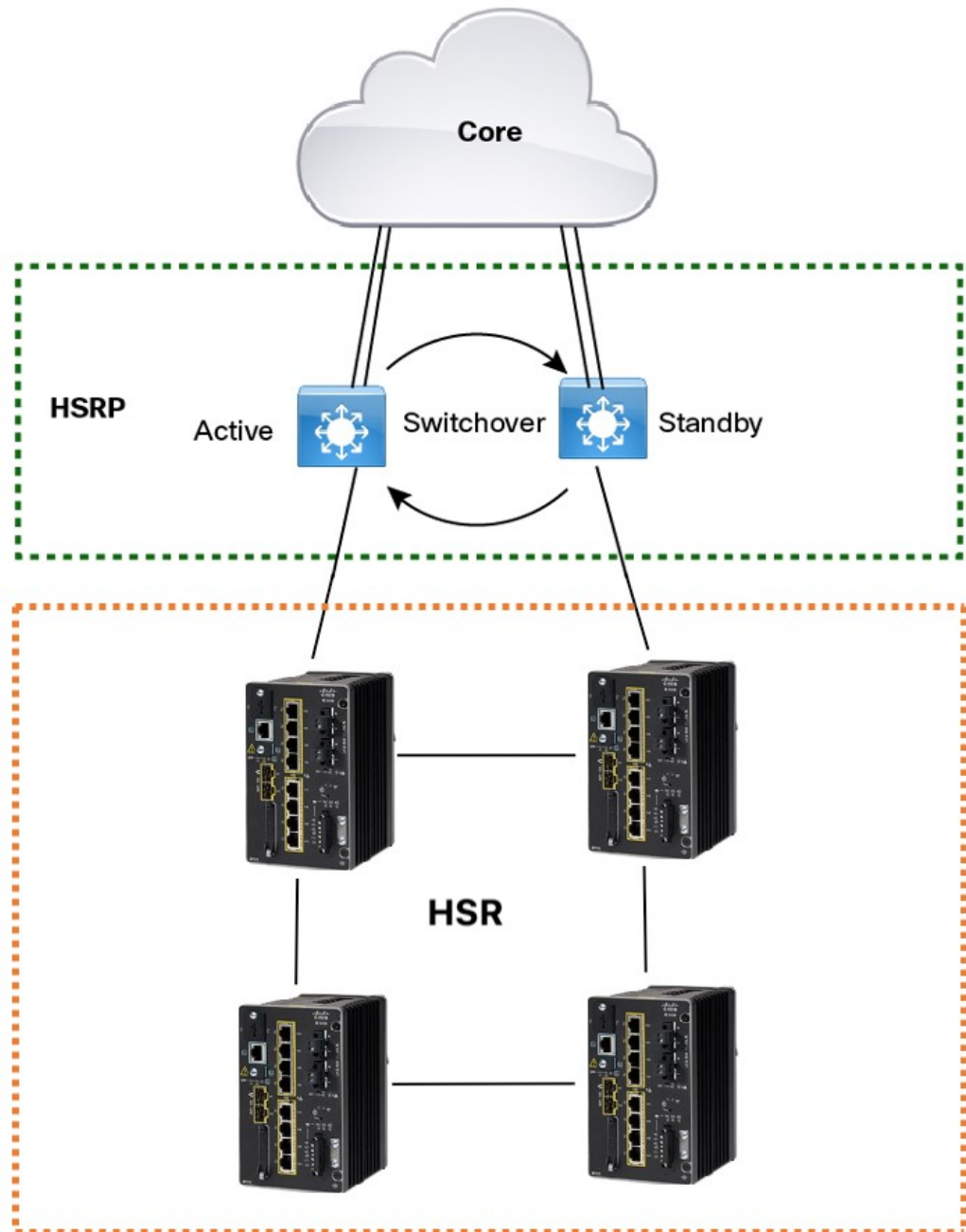
To implement HSR Uplink Redundancy, ensure that the **fpgamode-DualUplinkEnhancement** feature is not disabled. This feature is required to support the connectivity to a dual router (HSRP in this case) on the distribution layer:

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

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

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches ■

19

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

HSRP Configuration

The following example HSRP configuration applies to the two distribution switches Active & Standby in the above figure. In the following configuration, HSRP is configured in a Switch Virtual Interface (SVI).

```
Active# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Active(config)# interface vlan 10
Active(config-if)# ip address 30.30.30.2 255.255.255.0
Active(config-if)# standby 1 ip 30.30.30.1
Active(config-if)# standby 1 priority 120
Active(config-if)# end

Standby# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Standby(config)# interface Vlan10
Standby(config-if)# ip address 30.30.30.4 255.255.255.0
Standby(config-if)# standby 1 ip 30.30.30.1
Standby(config-if)# end

Active# show standby
Vlan10 - Group 1
  State is Active
    8 state changes, last state change 00:03:55
    Track object 1 (unknown)
  Virtual IP address is 30.30.30.1
  Active virtual MAC address is 0000.0c07.ac01 (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 200 msec, hold time 750 msec
    Next hello sent in 0.176 secs
  Preemption enabled, delay min 5 secs, reload 5 secs, sync 5 secs
  Active router is local
  Standby router is 30.30.30.4, priority 100 (expires in 0.656 sec)
  Priority 120 (configured 120)
  Group name is "hsrp-Vl10-1" (default)
  FLAGS: 0/1
Active# show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl10        1    120 P Active  local           30.30.30.4      30.30.30.1


Standby# show standby
Vlan10 - Group 1
  State is Standby
    13 state changes, last state change 00:04:17
    Track object 1 (unknown)
  Virtual IP address is 30.30.30.1
  Active virtual MAC address is 0000.0c07.ac01 (MAC Not In Use)
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 200 msec, hold time 750 msec
    Next hello sent in 0.064 secs
  Preemption enabled, delay min 5 secs, reload 5 secs, sync 5 secs
  Active router is 30.30.30.2, priority 120 (expires in 0.816 sec)
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Vl10-1" (default)
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

20

```
   FLAGS: 0/1
Standby# show standby brief
                      P indicates configured to preempt.
                      |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl10        1    100 P Standby 30.30.30.2      local           30.30.30.1
```

Guidelines and Limitations

- HSR-SAN and HSR-PRP are supported only on the following IE 3400 and IE 3400H Series switches:

    - Advanced System IE-3400-8P2S

    - Advanced System IE-3400-8T2S

    - All IE 3400H Series SKUs

    - For HSR-PRP, these expansion modules can host the PRP interface: IEM-3400-8T, IEM-3400-8S, and IEM-3400-8P

- HSR-SAN (Single RedBox mode) and HSR-PRP (Dual RedBox mode) are the only HSR modes supported.

- Only 1 HSR instance is supported. Note that the switch supports only 1 HSR or 1 PRP instance, so if a PRP instance has been created, no HSR instance can be created.

- HSR ring 1 can only be configured as a pair of ports: G1/1 and G1/2 or G1/3 and G1/4. Using these port pairs, you can configure 1 HSR ring.

- The HSR feature requires the Network Essential license.

- The HSR feature is not enabled by default and you must explicitly configure the HSR rings.

- HSR is disabled automatically if the required firmware image is not available on the system.

- The recommended maximum number of nodes in the node table is 512. Nodes are all the DANH and VDAN devices that can be connected to the ring at same time. This number is not an absolute limit, but higher numbers of entries may increase the number of duplicate packets received by the end devices.

- The maximum number of nodes in the HSR ring is 50.

- HSR ring ports can only be configured in L2 mode.

- HSR is supported on following port types:

    - 100 mbps, Full Duplex. Half duplex is not supported.

    - 1000 mbps, Full Duplex. Half duplex is not supported.

    - Both ports of one ring must be of same speed and type (that is, both can be SFPs or both can be copper)

- The following protocols and features are are mutually exclusive with HSR on the same port:

    - PRP

    - EtherChannels

    - Link Aggregation Control Protocol (LACP)

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

21

> > • Port Aggregation Protocol (PAgP)
>
> > • Resilient Ethernet Protocol (REP)

- The HSR feature does not work together with L2NAT.

- MACsec, HSR, and PRP are not allowed together.

- HSR supports an MTU size of up to 1998 bytes of Ethernet payload.

- STP is not supported on the HSR ring. By default, all modes of Spanning Tree Protocol (STP) will be disabled on the ring ports.

- PTP over HSR-SAN is supported on IE3400 Advanced FPGA SKUs and IE 3400H. PTP over HSR-SAN is not supported on IE3200 or IE3300.

- Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) are not supported on HSR. That is, SPAN and RSPAN should not be used to monitor the traffic on an HSR ring. In addition, traffic that has been monitored using RSPAN should not be transferred over an HSR ring.

- It is important for all interfaces in an HSR ring to have the same speed and duplex settings. It is recommended to apply those settings before configuring ring membership.

- Once a port is part of ring, the port cannot be shut down.

  For example, if G1/3 and G1/4 are part of an HSR ring and you try to shut down G1/3 or G1/4, the operation will not be permitted:

  ```
  Switch(config)# interface range g1/3
  Switch(config-if-range)#shutdown
   %Interface GigabitEthernet1/3 is configured in a HSR ring shutdown not permitted!
  Switch(config-if-range)#
  ```

  You can perform a shutdown of the HSR ring. For example:

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

- VLAN configuration such as trunk and access mode must be the same on both the ports participating in the ring. For example, if G1/4 and G1/3 in an HSR ring are in trunk mode and you attempt to change the mode of one port to access, the ports in the ring will not be bundled:

  ```
  Switch(config)# interface range g1/3
  Switch(config-if-range)# switchport mode  access
  Jul 27 22:00:27.809 IST: %EC-5-CANNOT_BUNDLE2: Gi1/3 is not compatible with Gi1/4 and
  will be suspended (trunk mode of Gi1/3 is access, Gi1/4 is dynamic)
  ```

- After an interface is added in the HSR ring, only the primary interface counters are updated. You should not need to configure and check the status of individual physical interfaces after they are added to the HSR ring.

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

  ```
  Switch1(config)# interface range g1/1-2
  Switch1(config-if-range)# shutdown
  Switch1(config-if-range)# hsr-ring hs1
  ```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

22

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

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

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

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

HSR-PRP Dual RedBox mode

- The 2 ports connected to the HSR ring must be Gi1/1 and Gi1/2, and the port connected to the PRP network can be any other port from the base module or expansion module. All remaining ports are available for normal use.

- PRP configuration is not required on the port that connects to PRP LAN A or LAN B.

- HSR ring members and the port connecting to PRP LAN A or LAN B should be in the same VLAN.

- When HSR-PRP RedBox mode is disabled, the two fixed ports that were part of HSR-PRP are moved to the default configuration.

- HSR Ring 1 is configured when HSR-PRP is enabled.

- The CLI command **hsr-prp-mode enable prp-lan-a | prp-lan-b** to enable HSR-PRP works without the Net Id option and the default value is 1.

  For multiple PRP networks, you can use the Net Id option with a value of 1 through 6. The CLI command is **hsr-prp-mode enable prp-lan-a | prp-lan-b <netid>**.

- Devices from LAN-A and LAN-B should not have direct connections. Connections should be through either Dual RedBox A or B or through PRP RedBox.

- Devices should not be connected directly to both PRP networks (LAN A and LAN B) at the same time.

- The maximum number of VDAN table and node table entries supported is 512 for HSR.

- You can shut down an HSR ring interface but you cannot remove the HSR interface when HSR-PRP is configured.

- HSR-PRP supported in both the default and redundancy FPGA profiles.

- A RedBox configured as HSR-PRP LAN A must be connected to the PRP LAN A network, and a RedBox configured as HSR-PRP LAN B must be connected to the PRP LAN B network. If not, a warning message is displayed.

  All the non-HSR ports on the HSR-PRP RedBox are considered to be within the same LAN, LAN A or LAN B, according to the mode of configuration of the HSR-PRP RedBox.

- MACSec is not supported in HSR-PRP.

- PTP over HSR-PRP is not supported.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

23

- The **show run** command does not show **hsr-ring 1** under interface configurations when HSR-PRP is enabled.

- SAN devices between LAN-A and LAN-B are required to be isolated from each other. This means that the HSR-PRP dual RedBoxes and any of their connected devices cannot ping each other across the two isolated LANs.

- The Syslog message "wrong LAN ID" is displayed based on the hardware statistics. If some other node in the PRP LAN is connected to the wrong LAN and it is sending the wrong LAN ID, this will cause the hardware to increment the statistics count as well.

Note   If there is a LAN ID mismatch, you are advised to check that the HSR-PRP RedBox has been configured and is connected to the same PRP network. For example, if the HSR-PRP RedBox is configured for HSR-PRP-LAN-A mode, the PRP port is connected to LAN-A.

- Uplink redundancy through HSRP is not supported when HSR-PRP is enabled.

- When HSR-PRP is configured, **hsr-ring 1** is not displayed under the associated physical interfaces in the running configuration.

- As with HSR-SAN, when you remove HSR-PRP, the corresponding associated physical interfaces will move to shutdown state.

- When configuring or removing HSR-SAN or HSR-PRP, a warning message appears to notify you that the ports will move to shutdown state when HSR-PRP is disabled. The warning is followed by a prompt (yes/no) for you to confirm the port shutdown.

PTP over HSR

- PTP over HSR is supported only for the PTP Power profile.

- PTP over HSR does not support Hybrid clock mode. Only Boundary clock and transparent clock modes are supported.

- We recommend that you have identical PTP configuration on the interfaces that are part of the same HSR ring to allow for seamless transitions between PASSIVE_SLAVE and SLAVE states.

Default Settings

Table 1: HSR Ring Parameters

Parameter	Description	Range	Default Value
entryForgetTime	Time for clearing an inactive entry from duplicate discard table.	0-65535	400 ms
fpgamode-DualUplinkEnhancement	Set FPGA register for source mac filtering.	enable or disable	enable

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

24

Parameter	Description	Range	Default Value
nodeForgetTime	Time to clear an inactive entry from the node table.	0-65535	60000 ms
nodeRebootInterval	Time after which the RedBox must start sending supervision frames after bootup.	0-65535	500 ms
pauseFrameTime	Time interval between HSR pause frames.	0-65535	25 ms
proxyNodeTableForgetTime	Time to clear an inactive entry from the proxy node table or vdan table.	0-65535	60000 ms
supervisionFrameLifeCheckInterval	Life check interval value for supervision frames.	0-65535	2000 ms
supervisionFrameOption			
mac-da	The last bytes of the destination MAC address of supervision frames (01:15:4E:00:01:00). The last 00 is replaced by the value of this parameter.	1-255 MAC DA last eight bits option value	No default
vlan-cfi	Enable Canonical Format Indicator (CFI) for the VLAN tagged frame.	enable or disable	disable
vlan-cos	Class of Service (COS) value to be set in the VLAN tag of the Supervision frame.	0-7	0
vlan-id	The VLAN tag of the supervision frame.	0-4095	0
vlan-tagged	Set VLAN tagging option.	enable or disable	disable
supervisionFrameRedboxMacaddress	The RedBox MAC address in the supervision frames.	48-bit RedBox MAC address	The interface HSR ring MAC address
supervisionFrameTime	Time interval between supervision frames.	0-65535	3 ms

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

25

Configuring an HSR Ring

Follow these steps to configure an HSR ring:

Before you begin

- See Guidelines and Limitations, on page 21.

- Ensure that the member interfaces of a HSR ring are not participating in any redundancy protocols such as FlexLinks, EtherChannel, REP, and so on before configuring a HSR ring.

Step 1 Enter global configuration mode:

```
Switch# configure terminal
```

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

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

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

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

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

```
Switch(config)# interface range gigabitEthernet 1/1-2
Switch(config-if-range)# no ptp enable
```

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

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

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

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

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

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

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

```
Switch(config)# interface range gigabitEthernet 1/1-2
Switch(config-if-range)# hsr-ring 1
```

Step 9 (Optional) If required, configure HSR ring optional parameters. See Default Settings, on page 24 for the parameter descriptions, ranges and default values.

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

Step 10 Turn on the HSR interface:

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

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

26

Example

```
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface range gigabitEthernet 1/1-2
Switch(config-if-range)# no ptp enable
Switch(config-if-range)# shutdown
Switch(config-if-range)# hsr-ring 1
Switch(config-if-range)# hsr-ring 1 supervisionFrameLifeCheckInterval 10000
Switch(config-if-range)# no shutdown
Switch(config-if-range)# end
```

Configuring HSR-PRP

Follow these steps to enable HSR-PRP Redbox mode on the switch. Enabling HSR-PRP mode creates an HSR ring and bridges the the HSR ring to a PRP network.

Before you begin

- See .

SUMMARY STEPS

1. Enter global configuration mode:
2. Enable HSR-PRP mode and select LAN A or LAN B and the optional PRP Net ID:

DETAILED STEPS

Step 1 Enter global configuration mode:

```
IE3400# configure terminal
```

Step 2 Enable HSR-PRP mode and select LAN A or LAN B and the optional PRP Net ID:

hsr-prp-mode enable {prp-lan-a | prp-lan-b} [1-6]

- prp-lan-a: Redbox is connected to LAN A.

- prp-lan-b: Redbox is connected to LAN B.

- 1-6: PRP Net ID value from 1 to 6.

  The default is 1.

  Note Be sure to configure the same Net ID in Redbox A and B that is part of the same PRP network.

Example:

```
IE3400(config)#hsr-prp-mode enable prp-lan-a
```

To disable HSR-PRP Redbox mode, use the command **no hsr-prp-mode enable**.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

27

Enabling HSR Alarms

To enable alarms for HSR, follow these steps:

Before you begin

Alarms and actions can be enabled/disabled at the facility level only. You cannot enable only partial faults or full faults; either all alarms for given facility are enabled or all are disabled.

See HSR Alarms, on page 16 for details about HSR alarms.

SUMMARY STEPS

1. Enter global configuration mode:
2. Enable the HSR alarm facility:
3. (Optional) Enable SNMP notification for HSR alarms:
4. (Optional) Associate HSR alarms with the Major Relay:
5. (Optional) Send HSR alarms to a syslog server:
6. (Optional) Enable logging of informational HSR alarm messages:
7. Exit global configuration mode:
8. Verify the configuration:

DETAILED STEPS

Step 1   Enter global configuration mode:

```
Switch# configure terminal
```

Step 2   Enable the HSR alarm facility:

```
Switch(config)# alarm facility hsr enable
```

To disable HSR alarms, enter **no alarm facility hsr enable**.

Step 3   (Optional) Enable SNMP notification for HSR alarms:

```
Switch(config)# alarm facility hsr notifies
```

Step 4   (Optional) Associate HSR alarms with the Major Relay:

```
Switch(config)# alarm facility hsr relay major
```

Step 5   (Optional) Send HSR alarms to a syslog server:

```
Switch(config)# alarm facility hsr syslog
```

Step 6   (Optional) Enable logging of informational HSR alarm messages:

```
Switch(config)# logging alarm informational
```

Step 7   Exit global configuration mode:

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

Step 8   Verify the configuration:

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

28

```
Switch# show facility-alarm status
```

Clearing All Node Table and VDAN Table Dynamic Entries

To clear all dynamic entries in the node table, enter

clear hsr node-table

To clear all dynamic entries in the VDAN table, enter

clear hsr vdan-table

Verifying Configuration

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

Configuration Example

HSR-SAN

This example shows the configuration of an HSR ring (Ring 1) using G1/3 and G1/4 ports between four devices.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

29
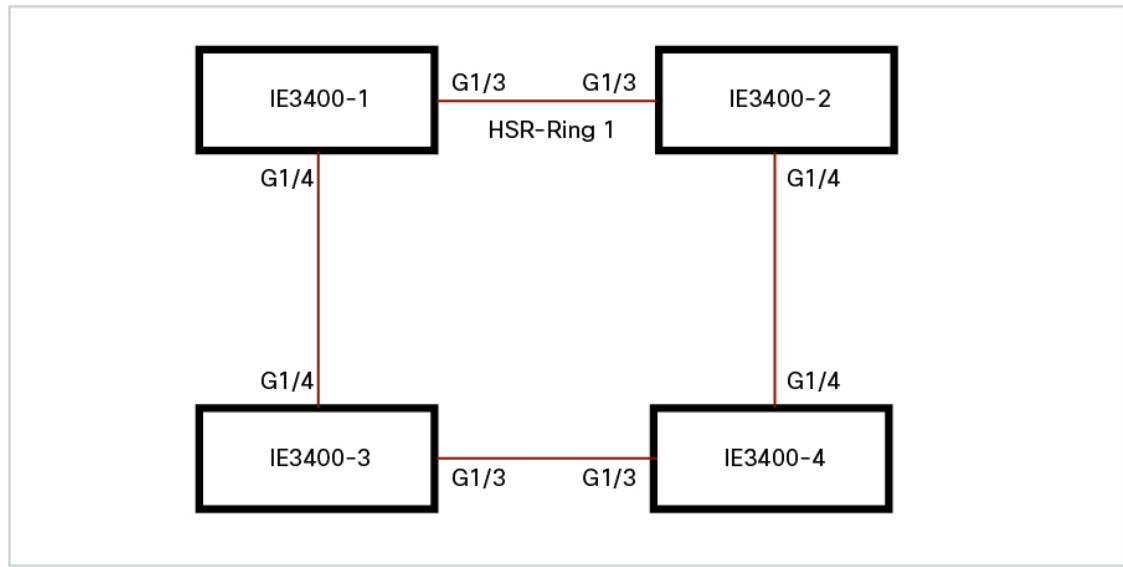
```
IE3400-1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IE3400-1(config)# interface range g1/3-4
IE3400-1(config-if-range)# shutdown
IE3400-1(config-if-range)# hsr-ring 1
IE3400-1(config-if-range)# no shutdown
IE3400-1(config-if-range)# end
IE3400-1#
IE3400-2# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IE3400-2(config)# interface range g1/3-4
IE3400-2(config-if-range)# shutdown
IE3400-2(config-if-range)# hsr-ring 1
IE3400-2(config-if-range)# no shutdown
IE3400-2(config-if-range)# end
IE3400-2#
IE3400-3# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IE3400-3(config)# interface range g1/3-4
IE3400-3(config-if-range)# shutdown
IE3400-3(config-if-range)# hsr-ring 1
IE3400-3(config-if-range)# no shutdown
IE3400-3(config-if-range)# end
IE3400-3#
IE3400-4# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IE3400-4(config)# interface range g1/3-4
IE3400-4(config-if-range)# shutdown
IE3400-4(config-if-range)# hsr-ring 1
IE3400-4(config-if-range)# no shutdown
IE3400-4(config-if-range)# end
IE3400-4#
IE3400-1# sh hsr ring 1 detail
HSR-ring: HS1
------------
 Layer type = L2
 Operation Mode = mode-H
 Ports: 2      Maxports = 2
 Port state = hsr-ring is Inuse
 Protocol = Enabled  Redbox Mode = hsr-san
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

30

```
                 Ports in the ring:
                   1) Port: Gi1/3
                     Logical slot/port = 1/3      Port state = Inuse
                         Protocol = Enabled
                   2) Port: Gi1/4
                     Logical slot/port = 1/4      Port state = Inuse
                         Protocol = Enabled

                 Ring Parameters:
                  Redbox MacAddr: f454.3365.8a84
                  Node Forget Time: 60000 ms
                  Node Reboot Interval: 500 ms
                  Entry Forget Time: 400 ms
                  Proxy Node Forget Time: 60000 ms
                  Supervision Frame COS option: 0
                  Supervision Frame CFI option: 0
                  Supervision Frame VLAN Tag option: Disabled
                  Supervision Frame MacDa: 0x00
                  Supervision Frame VLAN id: 0
                  Supervision Frame Time: 3 ms
                  Life Check Interval: 2000 ms
                  Pause Time: 25 ms

                 IE3400-2# show hsr ring 1 detail
                 HSR-ring: HS1
                 ------------
                  Layer type = L2
                  Operation Mode = mode-H
                  Ports: 2        Maxports = 2
                  Port state = hsr-ring is Inuse
                  Protocol = Enabled  Redbox Mode = hsr-san
                 Ports in the ring:
                   1) Port: Gi1/3
                     Logical slot/port = 1/3      Port state = Inuse
                         Protocol = Enabled
                   2) Port: Gi1/4
                     Logical slot/port = 1/4      Port state = Inuse
                         Protocol = Enabled

                 Ring Parameters:
                  Redbox MacAddr: 34c0.f958.ee83
                  Node Forget Time: 60000 ms
                  Node Reboot Interval: 500 ms
                  Entry Forget Time: 400 ms
                  Proxy Node Forget Time: 60000 ms
                  Supervision Frame COS option: 0
                  Supervision Frame CFI option: 0
                  Supervision Frame VLAN Tag option: Disabled
                  Supervision Frame MacDa: 0x00
                  Supervision Frame VLAN id: 0
                  Supervision Frame Time: 3 ms
                  Life Check Interval: 2000 ms
                  Pause Time: 25 ms

                 IE3400-4# sh hsr ring 1 de
                 HSR-ring: HS1
                 ------------
                  Layer type = L2
                  Operation Mode = mode-H
                  Ports: 2        Maxports = 2
                  Port state = hsr-ring is Inuse
                  Protocol = Enabled  Redbox Mode = hsr-san
                 Ports in the ring:
                   1) Port: Gi1/3
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

31

```
       Logical slot/port = 1/3      Port state = Inuse
             Protocol = Enabled
   2) Port: Gi1/4
       Logical slot/port = 1/4      Port state = Inuse
             Protocol = Enabled

Ring Parameters:
 Redbox MacAddr: f454.3312.5104
 Node Forget Time: 60000 ms
 Node Reboot Interval: 500 ms
 Entry Forget Time: 400 ms
 Proxy Node Forget Time: 60000 ms
 Supervision Frame COS option: 0
 Supervision Frame CFI option: 0
 Supervision Frame VLAN Tag option: Disabled
 Supervision Frame MacDa: 0x00
 Supervision Frame VLAN id: 0
 Supervision Frame Time: 3 ms
 Life Check Interval: 2000 ms
 Pause Time: 25 ms

IE3400-3# sh hsr ring 1 detail
HSR-ring: HS1
------------
 Layer type = L2
 Operation Mode = mode-H
 Ports: 2        Maxports = 2
 Port state = hsr-ring is Inuse
 Protocol = Enabled  Redbox Mode = hsr-san
Ports in the ring:
  1) Port: Gi1/3
      Logical slot/port = 1/3      Port state = Inuse
             Protocol = Enabled
   2) Port: Gi1/4
       Logical slot/port = 1/4      Port state = Inuse
             Protocol = Enabled

Ring Parameters:
 Redbox MacAddr: f454.335c.4684
 Node Forget Time: 60000 ms
 Node Reboot Interval: 500 ms
 Entry Forget Time: 400 ms
 Proxy Node Forget Time: 60000 ms
 Supervision Frame COS option: 0
 Supervision Frame CFI option: 0
 Supervision Frame VLAN Tag option: Disabled
 Supervision Frame MacDa: 0x00
 Supervision Frame VLAN id: 0
 Supervision Frame Time: 3 ms
 Life Check Interval: 2000 ms
 Pause Time: 25 ms
```

HSR-PRP

The following shows an example HSR-PRP configuration:

```
!
hsr-prp-mode enable prp-lan-a 1
!
interface HSR-ring1
switchport access vlan 80
switchport mode access
!
interface GigabitEthernet1/1
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

32

```
switchport access vlan 80
switchport mode access
!
interface GigabitEthernet1/2
switchport access vlan 80
switchport mode access
!
```

The following example shows output for **show** commands with HSR configured for HSR-PRP mode:

```
IE3400# show hsr ring 2 detail
HSR-ring: HS2
------------
Layer type = L2
Operation Mode = mode-H
Ports: 2        Maxports = 2
Port state = hsr-ring is Inuse
Protocol = Enabled  Redbox Mode = hsr-prp-lan-a  PathId = 1
Ports in the ring:
  1) Port: Gi1/1
   Logical slot/port = 1/1      Port state = Inuse
        Protocol = Enabled
  2) Port: Gi1/2
   Logical slot/port = 1/2      Port state = Inuse
        Protocol = Enabled

Ring Parameters:
Redbox MacAddr: 34c0.f958.e384
Node Forget Time: 60000 ms
Node Reboot Interval: 500 ms
Entry Forget Time: 400 ms
Proxy Node Forget Time: 60000 ms
Supervision Frame COS option: 0
Supervision Frame CFI option: 0
Supervision Frame VLAN Tag option: Disabled
Supervision Frame MacDa: 0x00
Supervision Frame VLAN id: 0
Supervision Frame Time: 3 ms
Life Check Interval: 2000 ms
Pause Time: 25 ms


IE3400#show hsr ?
  node-table  HSR Node Table
  ring        Ring information
  statistics  HSR Statistics information
  vdan-table  HSR VDAN Table

IE3400#show hsr node-table
HSR ring 1 Node Table
==================================
   Mac Address    Type    Dyn     TTL
---------------- -----   ---   -------
 ECCE.13EB.72A2  danh    Y      59
 ECCE.13EB.72A1  danh    Y      59
 A0E0.AF0E.0F01  danh    Y      59
 A0E0.AF0E.0F02  danh    Y      59
 E069.BAA3.2DE1  danh    Y      60
 E069.BAA3.2DE2  danh    Y      60
==================================
HSR ring 1 Total Entries: 6

IE3400#show hsr statistics ?
  egressPacketStatistics   Egress packet statistics
  ingressPacketStatistics  Ingress packet statistics
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

33

```
     nodeTableStatistics      Node table statistics
     pauseFrameStatistics     Pause frame statistics
     ptpPacketStatistics      PTP packet statistics
     wrongLanIdCount      Wrong LAN-ID packet statistics
IE3400#show hsr statistics ingressPacketStatistics
 HSR ring 1 INGRESS STATS:
   ingress pkt port A: 17298689
   ingress pkt port B: 18730898
   ingress crc port A: 0
   ingress crc port B: 0
   ingress danh pkt portAcpt: 1526824
   ingress danh pkt dscrd: 358095
   ingress supfrm rcv port A: 15645639
   ingress supfrm rcv port B: 16121959
   ingress overrun pkt port A: 0
   ingress overrun pkt port B: 0
   ingress byte port a: 1240088922
   ingress byte port b: 1502552754
ingress wrong lan id c: 0

IE3400#show hsr statistics egressPacketStatistics
 HSR ring 1 EGRESS STATS:
   duplicate packets: 4336811
   supervision frames: 4425419
   packets sent on port A: 18089179
   packets sent on port B: 19794169
   byte sent on port a: 1453432770
   byte sent on port b: 1572795833


IE3400#show hsr vdan-table
HSR ring 1 VDAN Table
============================
   Mac Address    Dyn    TTL
---------------- --- -------
 E069.BAA3.2D22   N     -
 E069.BAA3.2D21   N     -
============================
HSR ring 1 Total Entries: 2

IE3400#show hsr ring 1 ?
  detail    Detail information
  status    HSR-ring status
  summary   Summary per hsr ring

IE3400#show hsr ring 1 detail
HSR-ring: HS1
------------
 Layer type = L2
 Operation Mode = mode-H
 Ports: 2 Maxports = 2
 Port state = hsr-ring is In use
 Protocol = Enabled   Redbox Mode = prp-lan-b   PathId = 0
Ports in the ring:
 1) Port: Gi1/1
   Logical slot/port = 1/1 Port state = In use
 Protocol = Enabled
 2) Port: Gi1/2
   Logical slot/port = 1/2 Port state = In use
 Protocol = Enabled

Ring Parameters:
 Redbox MacAddr: e069.baa3.2d22
 Node Forget Time: 60000 ms
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

34

```
   Node Reboot Interval: 500 ms
   Entry Forget Time: 400 ms
   Proxy Node Forget Time: 60000 ms
   Supervision Frame COS option: 0
   Supervision Frame CFI option: 0
   Supervision Frame VLAN Tag option: Disabled
   Supervision Frame MacDa: 0x00
   Supervision Frame VLAN id: 0
   Supervision Frame Time: 3 ms
   Life Check Interval: 1600 ms
   Pause Time: 25 ms
   fpgamode-DualUplinkEnhancement: Enabled

IE3400#show hsr ring 1 ?
  detail    Detail information
  status    HSR-ring status
  summary   Summary per hsr ring

IE3400#show hsr ring 1 status
HSR-ring: HS1
------------
 Port state = hsr-ring is In use
 Protocol = Enabled  Redbox Mode = prp-lan-b  PathId = 0
IE3400#show hsr ring 1 summa
IE3400#show hsr ring 1 summary
Flags:  D - down       H - bundled in HSR-ring
        R - Layer3     S - Layer2
        U - in use     s - suspended

Number of hsr-rings in use: 1
Group   HSR-ring     Ports
------+------------+---------------------------------------
1      HS1(SU)      Gi1/1(H), Gi1/2(H)

IE3400#
```

Related Documents

- Cisco Catalyst IE3400 Heavy Duty Series

- Cisco Catalyst IE3400 Rugged Series

- IEC 62439-3, Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)

Feature History

Feature Name	Release	Feature Information
HSR-PRP (Dual RedBox Mode)	Cisco IOS XE 17.14.1	Initial support on IE 3400 and IE 3400H.
PTP over HSR-SAN	Cisco IOS XE 17.4.1	Initial support on IE 3400 and IE 3400H.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

35

Feature Name	Release	Feature Information
High-Availability Seamless Redundancy (HSR) - HSR-SAN (Single Redbox Mode)	Cisco IOS XE 17.3.1	Initial support on IE 3400 and IE 3400H.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

36

Configuring HSRP

This chapter describes how to use Hot Standby Router Protocol (HSRP) to provide routing redundancy for routing IP traffic without being dependent on the availability of any single router.

Configuring HSRP

This chapter describes how to use Hot Standby Router Protocol (HSRP) to provide routing redundancy for routing IP traffic without being dependent on the availability of any single router.

Information About Configuring HSRP

HSRP Overview

HSRP is Cisco's standard method of providing high network availability by providing first-hop redundancy for IP hosts on an IEEE 802 LAN configured with a default gateway IP address. HSRP routes IP traffic without relying on the availability of any single router. It enables a set of router interfaces to work together to present the appearance of a single virtual router or default gateway to the hosts on a LAN. When HSRP is configured on a network or segment, it provides a virtual Media Access Control (MAC) address and an IP address that is shared among a group of configured routers. HSRP allows two or more HSRP-configured routers to use the MAC address and IP network address of a virtual router. The virtual router does not exist; it represents the common target for routers that are configured to provide backup to each other. One of the routers is selected to be the active router and another to be the standby router, which assumes control of the group MAC address and IP address should the designated active router fail.

Note   Routers in an HSRP group can be any router interface that supports HSRP, including routed ports and switch virtual interfaces (SVIs).

HSRP provides high network availability by providing redundancy for IP traffic from hosts on networks. In a group of router interfaces, the active router is the router of choice for routing packets; the standby router is the router that takes over the routing duties when an active router fails or when preset conditions are met.

HSRP is useful for hosts that do not support a router discovery protocol and cannot switch to a new router when their selected router reloads or loses power. When HSRP is configured on a network segment, it provides

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

37

a virtual MAC address and an IP address that is shared among router interfaces in a group of router interfaces running HSRP. The router selected by the protocol to be the active router receives and routes packets destined for the group's MAC address. For n routers running HSRP, there are n +1 IP and MAC addresses assigned.

HSRP detects when the designated active router fails, and a selected standby router assumes control of the Hot Standby group's MAC and IP addresses. A new standby router is also selected at that time. Devices running HSRP send and receive multicast UDP-based hello packets to detect router failure and to designate active and standby routers. When HSRP is configured on an interface, Internet Control Message Protocol (ICMP) redirect messages are automatically enabled for the interface.

You can configure multiple Hot Standby groups among switches and switch stacks that are operating in Layer 3 to make more use of the redundant routers.

To do so, specify a group number for each Hot Standby command group you configure for an interface. For example, you might configure an interface on switch 1 as an active router and one on switch 2 as a standby router and also configure another interface on switch 2 as an active router with another interface on switch 1 as its standby router.

The following figure shows a segment of a network configured for HSRP. Each router is configured with the MAC address and IP network address of the virtual router. Instead of configuring hosts on the network with the IP address of Router A, you configure them with the IP address of the virtual router as their default router. When Host C sends packets to Host B, it sends them to the MAC address of the virtual router. If for any reason, Router A stops transferring packets, Router B responds to the virtual IP address and virtual MAC address and becomes the active router, assuming the active router duties. Host C continues to use the IP address of the virtual router to address packets destined for Host B, which Router B now receives and sends to Host B. Until Router A resumes operation, HSRP allows Router B to provide uninterrupted service to users on Host C's segment that need to communicate with users on Host B's segment and also continues to perform its normal function of handling packets between the Host A segment and Host B.

Figure 2: Typical HSRP Configuration

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

38
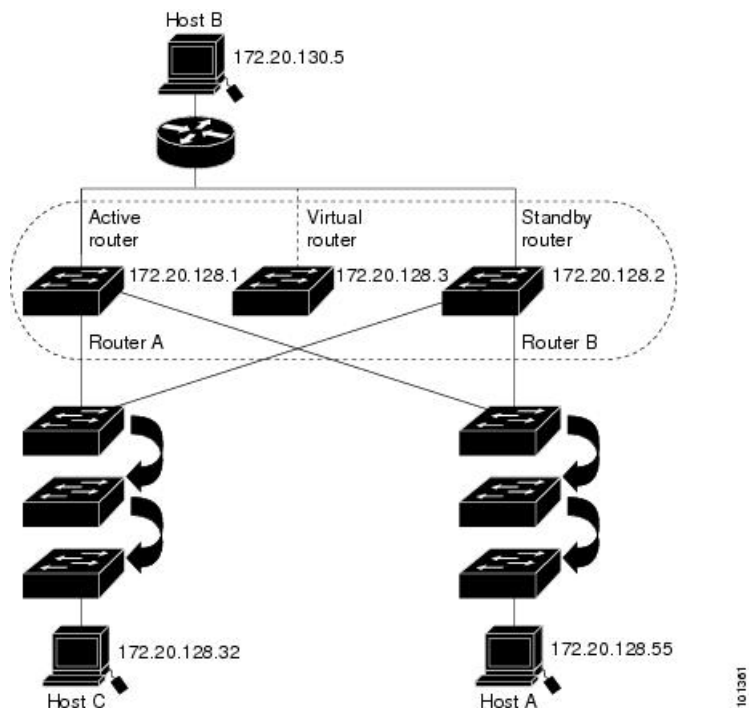
HSRP Versions

The switch supports these HSRP versions:

- HSRPv1- Version 1 of the HSRP, the default version of HSRP. It has these features:

  - The HSRP group number can be from 0 to 255.

  - HSRPv1 uses the multicast address 224.0.0.2 to send hello packets, which can conflict with Cisco Group Management Protocol (CGMP) leave processing. You cannot enable HSRPv1 and CGMP at the same time; they are mutually exclusive.

- HSRPv2- Version 2 of the HSRP has these features:

  - HSRPv2 uses the multicast address 224.0.0.102 to send hello packets. HSRPv2 and CGMP leave processing are no longer mutually exclusive, and both can be enabled at the same time.

  - HSRPv2 has a different packet format than HRSPv1.

A switch running HSRPv1 cannot identify the physical router that sent a hello packet because the source MAC address of the router is the virtual MAC address.

HSRPv2 has a different packet format than HSRPv1. A HSRPv2 packet uses the type-length-value (TLV) format and has a 6-byte identifier field with the MAC address of the physical router that sent the packet.

If an interface running HSRPv1 gets an HSRPv2 packet, the type field is ignored.

Multiple HSRP

The switch supports Multiple HSRP (MHSRP), an extension of HSRP that allows load sharing between two or more HSRP groups. You can configure MHSRP to achieve load-balancing and to use two or more standby groups (and paths) from a host network to a server network.

In the figure below, half the clients are configured for Router A, and half the clients are configured for Router B. Together, the configuration for Routers A and B establishes two HSRP groups. For group 1, Router A is the default active router because it has the assigned highest priority, and Router B is the standby router. For group 2, Router B is the default active router because it has the assigned highest priority, and Router A is the standby router. During normal operation, the two routers share the IP traffic load. When either router becomes unavailable, the other router becomes active and assumes the packet-transfer functions of the router that is unavailable.

Note   For MHSRP, you need to enter the **standby preempt** interface configuration command on the HSRP interfaces so that if a router fails and then comes back up, preemption restores load sharing.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

39

Figure 3: MHSRP Load Sharing
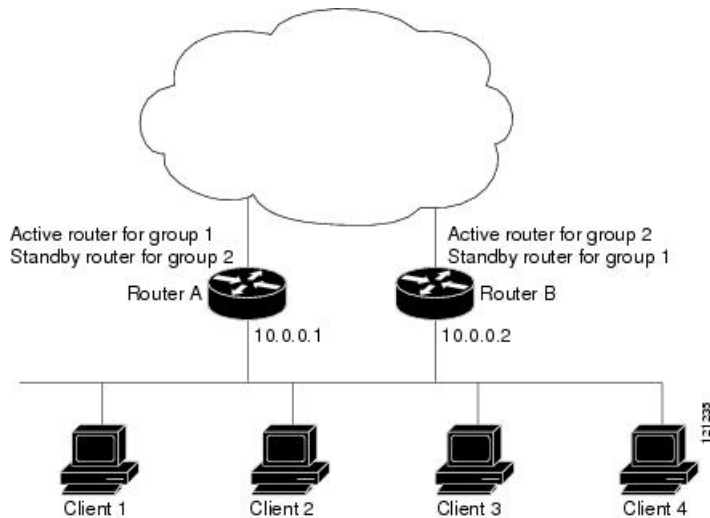
HSRP and Switch Stacks

HSRP hello messages are generated by the stack master. If an HSRP-active stack master fails, a flap in the HSRP active state might occur. This is because HSRP hello messages are not generated while a new stack master is elected and initialized, and the standby router might become active after the stack master fails.

Configuring HSRP for IPv6

Switches running the support the Hot Standby Router Protocol (HSRP) for IPv6. HSRP provides routing redundancy for routing IPv6 traffic not dependent on the availability of any single router. IPv6 hosts learn of available routers through IPv6 neighbor discovery router advertisement messages. These messages are multicast periodically or are solicited by hosts.

An HSRP IPv6 group has a virtual MAC address that is derived from the HSRP group number and a virtual IPv6 link-local address that is, by default, derived from the HSRP virtual MAC address.

Periodic messages are sent for the HSRP virtual IPv6 link-local address when the HSRP group is active. These messages stop after a final one is sent when the group leaves the active state.

Note When configuring HSRP for IPv6, you must enable HSRP version 2 (HSRPv2) on the interface.

HSRP IPv6 Virtual MAC Address Range

HSRP IPv6 uses a different virtual MAC address block than does HSRP for IP:

0005.73A0.0000 through 0005.73A0.0FFF (4096 addresses)

HSRP IPv6 UDP Port Number

Port number 2029 has been assigned to HSRP IPv6.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

40

How to Configure HSRP

Default HSRP Configuration

Table 2: Default HSRP Configuration

Feature	Default Setting
HSRP version	Version 1
HSRP groups	None configured
Standby group number	0
Standby MAC address	System assigned as: 0000.0c07.acXX, where XX is the HSRP group number
Standby priority	100
Standby delay	0 (no delay)
Standby track interface priority	10
Standby hello time	3 seconds
Standby holdtime	10 seconds

HSRP Configuration Guidelines

- HSRPv2 and HSRPv1 are mutually exclusive. HSRPv2 is not interoperable with HSRPv1 on an interface and the reverse.

- In the procedures, the specified interface must be one of these Layer 3 interfaces:

  - Routed port: A physical port configured as a Layer 3 port by entering the **no switchport** command in interface configuration mode.

  - SVI: A VLAN interface created by using the **interface vlan** *vlan_id* in global configuration mode, and by default a Layer 3 interface.

  - Etherchannel port channel in Layer 3 mode: A port-channel logical interface created by using the **interface port-channel** *port-channel-number* in global configuration mode, and binding the Ethernet interface into the channel group.

- You can configure a maximum of 32 HSRP groups.

- All Layer 3 interfaces must have IP addresses assigned to them.

- HSRP millisecond timers are not supported.

Enabling HSRP

The **standby ip** interface configuration command activates HSRP on the configured interface. If an IP address is specified, that address is used as the designated address for the Hot Standby group. If no IP address is specified, the address is learned through the standby function. You must configure at least one Layer 3 port

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

41

on the LAN with the designated address. Configuring an IP address always overrides another designated address currently in use.

When the **standby ip** command is enabled on an interface and proxy ARP is enabled, if the interface's Hot Standby state is active, proxy ARP requests are answered using the Hot Standby group MAC address. If the interface is in a different state, proxy ARP responses are suppressed.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **standby version** { **1** | **2** }
4. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
5. **end**
6. **show standby** [*interface-id* [*group*]]
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** Switch(config)# **configure terminal**	Enters global configuration mode.
Step 2	**interface** *interface-id* **Example:** Switch(config)# **interface gigabitethernet1/0/1**	Enters interface configuration mode, and enter the Layer 3 interface on which you want to enable HSRP.
Step 3	**standby version** { **1**	**2** } **Example:** Switch(config-if)# **standby version 1**	(Optional) Configures the HSRP version on the interface. • 1- Selects HSRPv1. • 2- Selects HSRPv2. If you do not enter this command or do not specify a keyword, the interface runs the default HSRP version, HSRP v1.
Step 4	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] **Example:** Switch(config-if)# **standby 1 ip**	Creates (or enable) the HSRP group using its number and virtual IP address. • (Optional) group-number- The group number on the interface for which HSRP is being enabled. The range is 0 to 255; the default is 0. If there is only one HSRP group, you do not need to enter a group number. • (Optional on all but one interface) ip-address- The virtual IP address of the hot standby router interface. You must enter the virtual IP address for at least one of the interfaces; it can be learned on the other interfaces.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

42

	Command or Action	Purpose
		• (Optional) **secondary**- The IP address is a secondary hot standby router interface. If neither router is designated as a secondary or standby router and no priorities are set, the primary IP addresses are compared and the higher IP address is the active router, with the next highest as the standby router.
Step 5	**end** **Example:** Switch(config-if)# **end**	Returns to privileged EXEC mode
Step 6	**show standby** [*interface-id* [*group*]] **Example:** Switch # **show standby**	Verifies the configuration of the standby groups.
Step 7	**copy running-config startup-config** **Example:** Switch# **copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Enabling and Verifying an HSRP Group for IPv6 Operation

In this task, when you enter the **standby ipv6** command, a link-local address is generated from the link-local prefix, and a modified EUI-64 format interface identifier is generated in which the EUI-64 interface identifier is created from the relevant HSRP virtual MAC address.

A link-local address is an IPv6 unicast address that can be automatically configured on any interface using the link-local prefix FE80::/10 (1111 1110 10) and the interface identifier in the modified EUI-64 format. Link-local addresses are used in the stateless autoconfiguration process. Nodes on a local link can use link-local addresses to communicate; the nodes do not need site-local or globally unique addresses to communicate.

In IPv6, a device on the link advertises in RA messages any site-local and global prefixes, and its willingness to function as a default device for the link. RA messages are sent periodically and in response to router solicitation messages, which are sent by hosts at system startup.

A node on the link can automatically configure site-local and global IPv6 addresses by appending its interface identifier (64 bits) to the prefixes (64 bits) included in the RA messages. The resulting 128-bit IPv6 addresses configured by the node are then subjected to duplicate address detection to ensure their uniqueness on the link. If the prefixes advertised in the RA messages are globally unique, then the IPv6 addresses configured by the node are also guaranteed to be globally unique. Router solicitation messages, which have a value of 133 in the Type field of the ICMP packet header, are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled RA message.

To enabling and verifying an HSRP group for IPv6, perform this procedure:

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

43

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> **enable**	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# **configure terminal**	Enters global configuration mode.
Step 3	**ipv6 unicast-routing** **Example:** Device(config)# **ipv6 unicast-routing**	Enables the forwarding of IPv6 unicast datagrams. • The **ipv6 unicast-routing** command must be enabled for HSRP for IPv6 to work.
Step 4	**interface** *type* *number* **Example:** Device(config)# **interface GigabitEthernet 0/0/0**	Specifies an interface type and number, and places the device in interface configuration mode.
Step 5	**standby** [*group-number*] **ipv6** {*link-local-address* | **autoconfig**} **Example:** Device(config-if)# **standby 1 ipv6 autoconfig**	Activates the HSRP in IPv6.
Step 6	**standby** [*group-number*] **preempt** [**delay minimum** *seconds* | **reload** *seconds* | **sync** *seconds*] **Example:** Device(config-if)# **standby 1 preempt**	Configures HSRP preemption and preemption delay.
Step 7	**standby** [*group-number*] **priority** *priority* **Example:** Device(config-if)# **standby 1 priority 110**	Configures HSRP priority.
Step 8	**exit** **Example:** Device(config-if)# **exit**	Returns the device to privileged EXEC mode.
Step 9	**show standby** [*type number* [*group*]] [**all** | **brief**] **Example:** Device# **show standby**	Displays HSRP information.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

44

	Command or Action	Purpose
Step 10	**show ipv6 interface** [**brief**] [*interface-type interface-number*] [**prefix**] **Example:** Device# **show ipv6 interface GigabitEthernet 0/0/0**	Displays the usability status of interfaces configured for IPv6.

Configuring HSRP Priority

The **standby priority**, **standby preempt**, and **standby track** interface configuration commands are all used to set characteristics for finding active and standby routers and behavior regarding when a new active router takes over.

When configuring HSRP priority, follow these guidelines:

- Assigning a priority allows you to select the active and standby routers. If preemption is enabled, the router with the highest priority becomes the active router. If priorities are equal, the current active router does not change.

- The highest number (1 to 255) represents the highest priority (most likely to become the active router).

- When setting the priority, preempt, or both, you must specify at least one keyword (**priority**, **preempt**, or both)

- The priority of the device can change dynamically if an interface is configured with the **standby track** command and another interface on the router goes down.

- The **standby track** interface configuration command ties the router hot standby priority to the availability of its interfaces and is useful for tracking interfaces that are not configured for HSRP. When a tracked interface fails, the hot standby priority on the device on which tracking has been configured decreases by 10. If an interface is not tracked, its state changes do not affect the hot standby priority of the configured device. For each interface configured for hot standby, you can configure a separate list of interfaces to be tracked.

- The **standby track** *interface-priority* interface configuration command specifies how much to decrement the hot standby priority when a tracked interface goes down. When the interface comes back up, the priority is incremented by the same amount.

- When multiple tracked interfaces are down and *interface-priority* values have been configured, the configured priority decrements are cumulative. If tracked interfaces that were not configured with priority values fail, the default decrement is 10, and it is noncumulative.

- When routing is first enabled for the interface, it does not have a complete routing table. If it is configured to preempt, it becomes the active router, even though it is unable to provide adequate routing services. To solve this problem, configure a delay time to allow the router to update its routing table.

Beginning in privileged EXEC mode, use one or more of these steps to configure HSRP priority characteristics on an interface:

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches ■

45

3. **standby** [*group-number*] **priority***priority*
4. **standby** [*group-number*] **preempt** [**delay** [**minimum***seconds*] [**reload***seconds*] [**sync***seconds*]]
5. **standby** [*group-number*] **track** *type number* [*interface-priority*]
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	**Purpose**
Step 1	**configure terminal** **Example:** Switch # **configure terminal**	Enters global configuration mode.
Step 2	**interface** *interface-id* **Example:** Switch(config)# **interface gigabitethernet1/0/1**	Enters interface configuration mode, and enter the HSRP interface on which you want to set priority.
Step 3	**standby** [*group-number*] **priority***priority* **Example:** Switch(config-if)# **standby 120 priority 50**	Sets a **priority** value used in choosing the active router. The range is 1 to 255; the default priority is 100. The highest number represents the highest priority. • (Optional) group-number—The group number to which the command applies. Use the **no** form of the command to restore the default values.
Step 4	**standby** [*group-number*] **preempt** [**delay** [**minimum***seconds*] [**reload***seconds*] [**sync***seconds*]] **Example:** Switch(config-if)# **standby 1 preempt delay 300**	Configures the router to **preempt**, which means that when the local router has a higher priority than the active router, it becomes the active router. • (Optional) group-number-The group number to which the command applies. • (Optional) **delay minimum**—Set to cause the local router to postpone taking over the active role for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over). • (Optional) **delay reload**—Set to cause the local router to postpone taking over the active role after a reload for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over after a reload). • (Optional) **delay sync**—Set to cause the local router to postpone taking over the active role so that IP redundancy clients can reply (either with an ok or wait reply) for the number of seconds shown. The range is

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

46

	Command or Action	Purpose
		0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over). Use the **no** form of the command to restore the default values.
Step 5	**standby** [*group-number*] **track** *type number* [*interface-priority*] **Example:** Switch(config-if)# **standby track interface gigabitethernet1/1/1**	Configures an interface to track other interfaces so that if one of the other interfaces goes down, the device's Hot Standby priority is lowered. • (Optional) group-number- The group number to which the command applies. • type- Enter the interface type (combined with interface number) that is tracked. • number- Enter the interface number (combined with interface type) that is tracked. • (Optional) interface-priority- Enter the amount by which the hot standby priority for the router is decremented or incremented when the interface goes down or comes back up. The default value is 10.
Step 6	**end** **Example:** Switch(config-if)# **end**	Returns to privileged EXEC mode.
Step 7	**show running-config**	Verifies the configuration of the standby groups.
Step 8	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Configuring MHSRP

To enable MHSRP and load-balancing, you configure two routers as active routers for their groups, with virtual routers as standby routers as shown in the *MHSRP Load Sharing* figure in the Multiple HSRP section. You need to enter the **standby preempt** interface configuration command on each HSRP interface so that if a router fails and comes back up, the preemption occurs and restores load-balancing.

Router A is configured as the active router for group 1, and Router B is configured as the active router for group 2. The HSRP interface for Router A has an IP address of 10.0.0.1 with a group 1 standby priority of 110 (the default is 100). The HSRP interface for Router B has an IP address of 10.0.0.2 with a group 2 standby priority of 110.

Group 1 uses a virtual IP address of 10.0.0.3 and group 2 uses a virtual IP address of 10.0.0.4.

Configuring Router A

SUMMARY STEPS

      1.   **configure terminal**

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

47

2. **interface** *type number*
3. **no switchport**
4. **ip address** *ip-address mask*
5. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
6. **standby** [*group-number*] **priority** *priority*
7. **standby** [*group-number*] **preempt** [**delay** [**minimum** *seconds*] [**reload** *seconds*] [**sync** *seconds*]]
8. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
9. **standby** [*group-number*] **preempt** [**delay** [**minimum** *seconds*] [**reload** *seconds*] [**sync** *seconds*]]
10. **end**
11. **show running-config**
12. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** Switch # **configure terminal**	Enters global configuration mode.
Step 2	**interface** *type number* **Example:** Switch (config)# **interface gigabitethernet1/0/1**	Configures an interface type and enters interface configuration mode.
Step 3	**no switchport** **Example:** Switch (config)# **no switchport**	Switches an interface that is in Layer 2 mode into Layer 3 mode for Layer 3 configuration.
Step 4	**ip address** *ip-address mask* **Example:** Switch (config-if)# **ip address 10.0.0.1 255.255.255.0**	Specifies an IP address for an interface.
Step 5	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] **Example:** Switch (config-if)# **standby 1 ip 10.0.0.3**	Creates the HSRP group using its number and virtual IP address. • (Optional) *group-number*- The group number on the interface for which HSRP is being enabled. The range is 0 to 255; the default is 0. If there is only one HSRP group, you do not need to enter a group number. • (Optional on all but one interface) *ip-address*- The virtual IP address of the hot standby router interface. You must enter the virtual IP address for at least one of the interfaces; it can be learned on the other interfaces. • (Optional) **secondary**- The IP address is a secondary hot standby router interface. If neither router is designated as a secondary or standby router and no

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

48

	Command or Action	**Purpose**
		priorities are set, the primary IP addresses are compared and the higher IP address is the active router, with the next highest as the standby router.
Step 6	**standby** [*group-number*] **priority** *priority* **Example:** Switch(config-if)# **standby 1 priority 110**	Sets a **priority** value used in choosing the active router. The range is 1 to 255; the default priority is 100. The highest number represents the highest priority. • (Optional) *group-number*—The group number to which the command applies. Use the **no** form of the command to restore the default values.
Step 7	**standby** [*group-number*] **preempt** [**delay** [**minimum** *seconds*] [**reload** *seconds*] [**sync** *seconds*]] **Example:** Switch(config-if)# **standby 1 preempt delay 300**	Configures the router to **preempt**, which means that when the local router has a higher priority than the active router, it becomes the active router. • (Optional) group-number-The group number to which the command applies. • (Optional) **delay minimum**—Set to cause the local router to postpone taking over the active role for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over). • (Optional) **delay reload**—Set to cause the local router to postpone taking over the active role after a reload for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over after a reload). • (Optional) **delay sync**—Set to cause the local router to postpone taking over the active role so that IP redundancy clients can reply (either with an ok or wait reply) for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over). Use the **no** form of the command to restore the default values.
Step 8	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] **Example:** Switch (config-if)# **standby 2 ip 10.0.0.4**	Creates the HSRP group using its number and virtual IP address. • (Optional) *group-number*- The group number on the interface for which HSRP is being enabled. The range is 0 to 255; the default is 0. If there is only one HSRP group, you do not need to enter a group number.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

49

	Command or Action	Purpose
		• (Optional on all but one interface) *ip-address*- The virtual IP address of the hot standby router interface. You must enter the virtual IP address for at least one of the interfaces; it can be learned on the other interfaces. • (Optional) **secondary**- The IP address is a secondary hot standby router interface. If neither router is designated as a secondary or standby router and no priorities are set, the primary IP addresses are compared and the higher IP address is the active router, with the next highest as the standby router.
Step 9	**standby** [*group-number*] **preempt** [**delay** [**minimum** *seconds*] [**reload** *seconds*] [**sync** *seconds*]] **Example:** Switch(config-if)# **standby 2 preempt delay 300**	Configures the router to **preempt**, which means that when the local router has a higher priority than the active router, it becomes the active router. • (Optional) group-number-The group number to which the command applies. • (Optional) **delay minimum**—Set to cause the local router to postpone taking over the active role for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over). • (Optional) **delay reload**—Set to cause the local router to postpone taking over the active role after a reload for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over after a reload). • (Optional) **delay sync**—Set to cause the local router to postpone taking over the active role so that IP redundancy clients can reply (either with an ok or wait reply) for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over). Use the **no** form of the command to restore the default values.
Step 10	**end** **Example:** Switch(config-if)# **end**	Returns to privileged EXEC mode.
Step 11	**show running-config**	Verifies the configuration of the standby groups.
Step 12	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Configuring Router B

SUMMARY STEPS

1. **configure terminal**

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

50

2. **interface** *type number*
3. **no switchport**
4. **ip address** *ip-address mask*
5. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
6. **standby** [*group-number*] **priority** *priority*
7. **standby** [*group-number*] **preempt** [**delay** [**minimum** *seconds*] [**reload** *seconds*] [**sync** *seconds*]]
8. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
9. **standby** [*group-number*] **preempt** [**delay** [**minimum** *seconds*] [**reload** *seconds*] [**sync** *seconds*]]
10. **end**
11. **show running-config**
12. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	**Purpose**
Step 1	**configure terminal** Example: Switch # **configure terminal**	Enters global configuration mode.
Step 2	**interface** *type number* Example: Switch (config)# **interface gigabitethernet1/0/1**	Configures an interface type and enters interface configuration mode.
Step 3	**no switchport** Example: Switch (config)# **no switchport**	Switches an interface that is in Layer 2 mode into Layer 3 mode for Layer 3 configuration.
Step 4	**ip address** *ip-address mask* Example: Switch (config-if)# **ip address 10.0.0.2 255.255.255.0**	Specifies an IP address for an interface.
Step 5	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] Example: Switch (config-if)# **standby 1 ip 10.0.0.3**	Creates the HSRP group using its number and virtual IP address. • (Optional) *group-number*- The group number on the interface for which HSRP is being enabled. The range is 0 to 255; the default is 0. If there is only one HSRP group, you do not need to enter a group number. • (Optional on all but one interface) *ip-address*- The virtual IP address of the hot standby router interface. You must enter the virtual IP address for at least one of the interfaces; it can be learned on the other interfaces. • (Optional) **secondary**- The IP address is a secondary hot standby router interface. If neither router is designated as a secondary or standby router and no

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

51

	Command or Action	Purpose
		priorities are set, the primary IP addresses are compared and the higher IP address is the active router, with the next highest as the standby router.
Step 6	**standby** [*group-number*] **priority** *priority* **Example:** Switch(config-if)# **standby 2 priority 110**	Sets a **priority** value used in choosing the active router. The range is 1 to 255; the default priority is 100. The highest number represents the highest priority. • (Optional) *group-number*—The group number to which the command applies. Use the **no** form of the command to restore the default values.
Step 7	**standby** [*group-number*] **preempt** [**delay** [**minimum** *seconds*] [**reload** *seconds*] [**sync** *seconds*]] **Example:** Switch(config-if)# **standby 1 preempt delay 300**	Configures the router to **preempt**, which means that when the local router has a higher priority than the active router, it becomes the active router. • (Optional) group-number-The group number to which the command applies. • (Optional) **delay minimum**—Set to cause the local router to postpone taking over the active role for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over). • (Optional) **delay reload**—Set to cause the local router to postpone taking over the active role after a reload for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over after a reload). • (Optional) **delay sync**—Set to cause the local router to postpone taking over the active role so that IP redundancy clients can reply (either with an ok or wait reply) for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over). Use the **no** form of the command to restore the default values.
Step 8	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] **Example:** Switch (config-if)# **standby 2 ip 10.0.0.4**	Creates the HSRP group using its number and virtual IP address. • (Optional) *group-number*- The group number on the interface for which HSRP is being enabled. The range is 0 to 255; the default is 0. If there is only one HSRP group, you do not need to enter a group number. • (Optional on all but one interface) *ip-address*- The virtual IP address of the hot standby router interface.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

52

	Command or Action	**Purpose**
		You must enter the virtual IP address for at least one of the interfaces; it can be learned on the other interfaces.
		• (Optional) **secondary**- The IP address is a secondary hot standby router interface. If neither router is designated as a secondary or standby router and no priorities are set, the primary IP addresses are compared and the higher IP address is the active router, with the next highest as the standby router.
Step 9	**standby** [*group-number*] **preempt** [**delay** [**minimum** *seconds*] [**reload** *seconds*] [**sync** *seconds*]] **Example:** Switch(config-if)# **standby 2 preempt delay 300**	Configures the router to **preempt**, which means that when the local router has a higher priority than the active router, it becomes the active router. • (Optional) group-number-The group number to which the command applies. • (Optional) **delay minimum**—Set to cause the local router to postpone taking over the active role for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over) . • (Optional) **delay reload**—Set to cause the local router to postpone taking over the active role after a reload for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over after a reload). • (Optional) **delay sync**—Set to cause the local router to postpone taking over the active role so that IP redundancy clients can reply (either with an ok or wait reply) for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over). Use the **no** form of the command to restore the default values.
Step 10	**end** **Example:** Switch(config-if)# **end**	Returns to privileged EXEC mode.
Step 11	**show running-config**	Verifies the configuration of the standby groups.
Step 12	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

53

Configuring HSRP Authentication and Timers

You can optionally configure an HSRP authentication string or change the hello-time interval and holdtime.

When configuring these attributes, follow these guidelines:

- The authentication string is sent unencrypted in all HSRP messages. You must configure the same authentication string on all routers and access servers on a cable to ensure interoperation. Authentication mismatch prevents a device from learning the designated Hot Standby IP address and timer values from other routers configured with HSRP.

- Routers or access servers on which standby timer values are not configured can learn timer values from the active or standby router. The timers configured on an active router always override any other timer settings.

- All routers in a Hot Standby group should use the same timer values. Normally, the *holdtime* is greater than or equal to 3 times the *hellotime*.

Beginning in privileged EXEC mode, use one or more of these steps to configure HSRP authentication and timers on an interface:

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **standby** [*group-number*] **authentication** *string*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	**Purpose**
Step 1	**configure terminal** **Example:** Switch # **configure terminal**	Enters global configuration mode.
Step 2	**interface** *interface-id* **Example:** Switch(config) # **interface gigabitethernet1/0/1**	Enters interface configuration mode, and enter the HSRP interface on which you want to set priority.
Step 3	**standby** [*group-number*] **authentication** *string* **Example:** Switch(config-if) # **standby 1 authentication word**	(Optional) **authentication** *string*—Enter a string to be carried in all HSRP messages. The authentication string can be up to eight characters in length; the default string is **cisco**. (Optional) *group-number*—The group number to which the command applies.
Step 4	**end** **Example:**	Returns to privileged EXEC mode.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

54

	Command or Action	Purpose
	`Switch(config-if) # end`	
Step 5	**show running-config**	Verifies the configuration of the standby groups.
Step 6	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Enabling HSRP Support for ICMP Redirect Messages

SUMMARY STEPS

1. ICMP redirect messages are automatically enabled on interfaces configured with HSRP. ICMP is a network layer Internet protocol that provides message packets to report errors and other information relevant to IP processing. ICMP provides diagnostic functions, such as sending and directing error packets to the host. This feature filters outgoing ICMP redirect messages through HSRP, in which the next hop IP address might be changed to an HSRP virtual IP address.

DETAILED STEPS

	Command or Action	Purpose
Step 1	ICMP redirect messages are automatically enabled on interfaces configured with HSRP. ICMP is a network layer Internet protocol that provides message packets to report errors and other information relevant to IP processing. ICMP provides diagnostic functions, such as sending and directing error packets to the host. This feature filters outgoing ICMP redirect messages through HSRP, in which the next hop IP address might be changed to an HSRP virtual IP address.	

Verifying HSRP

Verifying HSRP Configurations

From privileged EXEC mode, use this command to display HSRP settings:

show standby [*interface-id* [*group*]] [**brief**] [**detail**]

You can display HSRP information for the whole switch, for a specific interface, for an HSRP group, or for an HSRP group on an interface. You can also specify whether to display a concise overview of HSRP information or detailed HSRP information. The default display is **detail**. If there are a large number of HSRP groups, using the **show standby** command without qualifiers can result in an unwieldy display.

Example

```
Switch #show standby
VLAN1 - Group 1
Local state is Standby, priority 105, may preempt
Hellotime 3 holdtime 10
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches ■

55

```
                          Next hello sent in 00:00:02.182
                          Hot standby IP address is 172.20.128.3 configured
                          Active router is 172.20.128.1 expires in 00:00:09
                          Standby router is local
                          Standby virtual mac address is 0000.0c07.ac01
                          Name is bbb

                          VLAN1 - Group 100
                          Local state is Standby, priority 105, may preempt
                          Hellotime 3 holdtime 10
                          Next hello sent in 00:00:02.262
                          Hot standby IP address is 172.20.138.51 configured
                          Active router is 172.20.128.1 expires in 00:00:09
                          Active router is local
                          Standby router is unknown expired
                          Standby virtual mac address is 0000.0c07.ac64
                          Name is test
```

Configuration Examples for Configuring HSRP

Enabling HSRP: Example

This example shows how to activate HSRP for group 1 on an interface. The IP address used by the hot standby group is learned by using HSRP.

✎

Note   This procedure is the minimum number of steps required to enable HSRP. Other configurations are optional.

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# end
Switch # show standby
```

Example: Configuration and Verification for an HSRP Group

The following example shows configuration and verification for an HSRP group for IPv6 that consists of Device1 and Device2. The **show standby** command is issued for each device to verify the device's configuration:

Device 1 configuration

```
interface FastEthernet0/0.100
description DATA VLAN for PCs
encapsulation dot1Q 100
ipv6 address 2001:DB8:CAFE:2100::BAD1:1010/64
standby version 2
standby 101 priority 120
standby 101 preempt delay minimum 30
standby 101 authentication ese
standby 101 track Serial0/1/0.17 90
standby 201 ipv6 autoconfig
standby 201 priority 120
standby 201 preempt delay minimum 30
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

56

```
standby 201 authentication ese
standby 201 track Serial0/1/0.17 90
Device1# show standby
FastEthernet0/0.100 - Group 101 (version 2)
State is Active
2 state changes, last state change 5w5d
Active virtual MAC address is 0000.0c9f.f065
Local virtual MAC address is 0000.0c9f.f065 (v2 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 2.296 secs
Authentication text "ese"
Preemption enabled, delay min 30 secs
Active router is local
Priority 120 (configured 120)
Track interface Serial0/1/0.17 state Up decrement 90
IP redundancy name is "hsrp-Fa0/0.100-101" (default)
FastEthernet0/0.100 - Group 201 (version 2)
State is Active
2 state changes, last state change 5w5d
Virtual IP address is FE80::5:73FF:FEA0:C9
Active virtual MAC address is 0005.73a0.00c9
Local virtual MAC address is 0005.73a0.00c9 (v2 IPv6 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 2.428 secs
Authentication text "ese"
Preemption enabled, delay min 30 secs
Active router is local
Standby router is FE80::20F:8FFF:FE37:3B70, priority 100 (expires in 7.856 sec)
Priority 120 (configured 120)
Track interface Serial0/1/0.17 state Up decrement 90
IP redundancy name is "hsrp-Fa0/0.100-201" (default)
```

Device 2 configuration

```
interface FastEthernet0/0.100
description DATA VLAN for Computers
encapsulation dot1Q 100
ipv6 address 2001:DB8:CAFE:2100::BAD1:1020/64
standby version 2
standby 101 preempt
standby 101 authentication ese
standby 201 ipv6 autoconfig
standby 201 preempt
standby 201 authentication ese
Device2# show standby
FastEthernet0/0.100 - Group 101 (version 2)
State is Standby
7 state changes, last state change 5w5d
Active virtual MAC address is 0000.0c9f.f065
Local virtual MAC address is 0000.0c9f.f065 (v2 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.936 secs
Authentication text "ese"
Preemption enabled
MAC address is 0012.7fc6.8f0c
Standby router is local
Priority 100 (default 100)
IP redundancy name is "hsrp-Fa0/0.100-101" (default)
FastEthernet0/0.100 - Group 201 (version 2)
State is Standby
7 state changes, last state change 5w5d
Virtual IP address is FE80::5:73FF:FEA0:C9
Active virtual MAC address is 0005.73a0.00c9
Local virtual MAC address is 0005.73a0.00c9 (v2 IPv6 default)
Hello time 3 sec, hold time 10 sec
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

57

```
Next hello sent in 0.936 secs
Authentication text "ese"
Preemption enabled
Active router is FE80::212:7FFF:FEC6:8F0C, priority 120 (expires in 7.548 sec)
MAC address is 0012.7fc6.8f0c
Standby router is local
Priority 100 (default 100)
IP redundancy name is "hsrp-Fa0/0.100-201" (default)
```

Configuring HSRP Priority: Example

This example activates a port, sets an IP address and a priority of 120 (higher than the default value), and waits for 300 seconds (5 minutes) before attempting to become the active router:

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby ip 172.20.128.3
Switch(config-if)# standby priority 120 preempt delay 300
Switch(config-if)# end
Switch # show standby
```

Configuring MHSRP: Example

This example shows how to enable the MHSRP configuration shown in the figure *MHSRP Load Sharing*

Router A Configuration

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.1 255.255.255.0
Switch(config-if)# standby ip 10.0.0.3
Switch(config-if)# standby 1 priority 110
Switch(config-if)#  standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)#  standby 2 preempt
Switch(config-if)# end
```

Router B Configuration

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.2 255.255.255.0
Switch(config-if)# standby ip 10.0.0.3
Switch(config-if)#  standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)# standby 2 priority 110
Switch(config-if)#  standby 2 preempt
Switch(config-if)# end
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

58

Configuring HSRP Authentication and Timer: Example

This example shows how to configure word as the authentication string required to allow Hot Standby routers in group 1 to interoperate:

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 authentication word
Switch(config-if)# end
```

This example shows how to set the timers on standby group 1 with the time between hello packets at 5 seconds and the time after which a router is considered down to be 15 seconds:

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# standby 1 timers 5 15
Switch(config-if)# end
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches ▪

59

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

60

CHAPTER 3

Media Redundancy Protocol (MRP)

Information About MRP

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

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

MRP is supported on the following switches:

- Cisco Catalyst IE3x00 Rugged Series Switches (IE3200, IE3300, and IE3400)

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

61

• Cisco Catalyst IE3400 Heavy Duty Series Switches

• Cisco Catalyst IE3100 Rugged Series Switches (IE3100 and IE3105)

Note MRP is not supported on Cisco Catalyst ESS3300 Switches.

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

MRP Modes

There are two modes of MRP supported on the switch; however, only one mode can be enabled to operate on the switch at any given time:

• PROFINET MRP mode—Deployed in a PROFINET environment, the switch is added and managed by Siemens Totally Integrated Automation (TIA) Framework. This is the default MRP mode if the MRP manager or client license is activated through the web interface or command line.

Note When managing the switch with TIA, do not use the CLI or WebUI to configure MRP.

• MRP Command-line interface (CLI) mode—This mode is managed by the Cisco IOS CLI and WebUI, a web-based user interface (UI).

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

Protocol Operation

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

On Cisco Catalyst IE3x00 and IE3100 Rugged Series and IE3400 Heavy-Duty Switches, certain nodes or all nodes in the ring can also be configured to start as a Media Redundancy Automanager (MRA). MRAs select one MRM among each other by using a voting protocol and a configured priority value. The remaining MRAs transition to the MRC role.

All MRM and MRC ring ports support the following states:

• Disabled: Ring ports drop all received frames.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

62

- Blocked: Ring ports drop all received frames except MRP control frames and some standard frames, for example, LLDP.

- Forwarding: Ring ports forward all received frames.

- Not Connected: The link is physically down or disconnected. (This state differs from the Disabled state, in which the MRP Port is manually disabled through software.)

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

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

- Left Ring: The connection (small blue square, top) on the MRM is in a blocked state (as shown by the two parallel lines) because no ports are disconnected.

- Right Ring: Two MRC connections (left and center small white squares) are in the disabled state because the link between them is broken, as marked by a red "x".

Figure 4: MRP Ring States
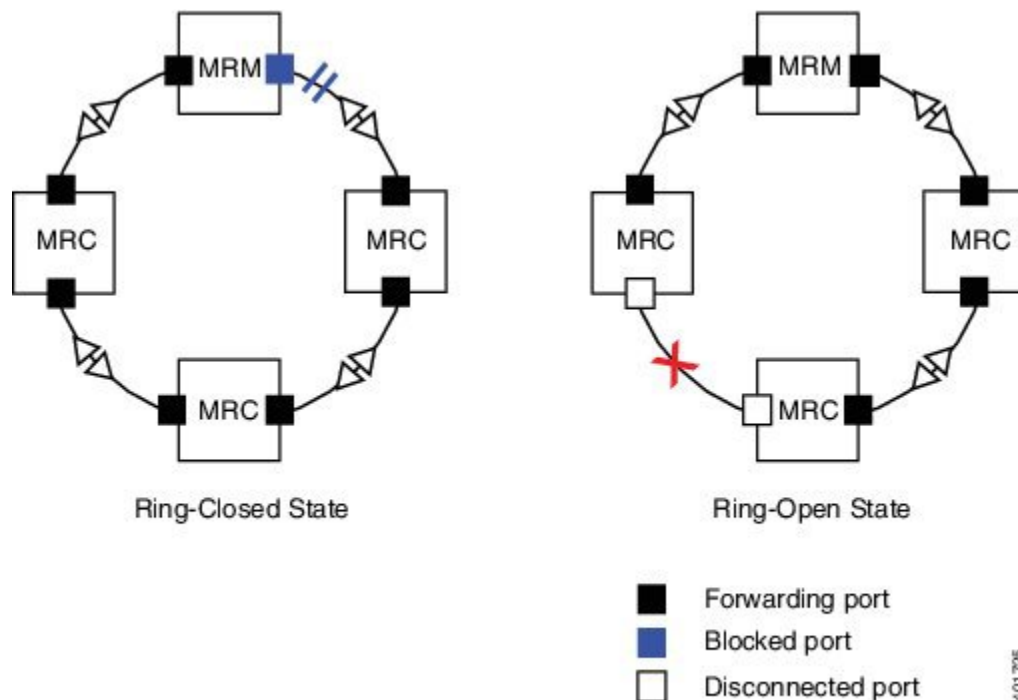
If a network failure occurs:

- The network shifts into the Ring-Open state.

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

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

63

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

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

MRP uses three types of control frames:

- To monitor the ring status, MRM regularly sends test frames on both ring ports.

- When MRM detects failure or recovery, it sends TopoChange frames on both ring ports.

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

Media Redundancy Automanager (MRA)

Note   MRA can be activated through the CLI or through PROFINET.

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

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

MRA functions as follows:

1. At power on, all MRAs begin the manager voting process. Each MRA begins to send MRP_Test frames on both ring ports. The MRP_Test frame contains the MRA's priority value. The remote manager's priority value contained in the received MRP_Test frames are compared with the MRA's own priority. If its own priority is higher than the received priority, the MRA sends a negative test manager acknowledgement (MRP_TestMgrNAck) frame, along with the remote manager's MAC address.

2. If the receiving MRA receives an MRP_TestMgrNAck with its own MAC address, the receiving MRA initiates the transition into the client (MRC) role.

3. The MRP_TestPropagate frame informs other MRA devices in the client role about the role change and the new higher priority manager. The clients receiving this frame update their higher priority manager information accordingly. This ensures that clients remain in the client role if the monitored higher priority manager role changes.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

64

License Levels

Note Information about the MRP feature license described below applies only to Cisco IOS XE releases earlier than 17.7.1. Use of MRP in Cisco IOS XE 17.7.1 and later does not require a feature license, only the Network Essentials Base license. Information below about Base Licenses and Add-On Licenses applies to all Cisco IOS XE releases.

In Cisco IOS XE releases prior to 17.7.1, use of the MRP feature requires a feature license. The feature license is enforced and must be authorized by Cisco before the feature can be enabled. To use the MRP feature, you buy an MRP feature license and Cisco installs an authorization code on your device at the time the device is purchased, or you can install the authorization code on your device using the **license smart authorization request add <feature-name> local** command.

In online mode, the device requests the license from the Cisco Smart Software Manager (CSSM) directly or through the Cisco Smart Licensing Utility (CSLU). The CSSM returns a smart license authorization code (SLAC) to the Product Instance (PI) directly or through the CSLU. If a device receives the authorization code, the smart agent on the device stores this authorization code in the tamper-proof trusted store and you can enable the feature. If you install the authorization code and do not enable the feature, when you boot the device the smart agent on the device will honor the auth-code that was stored in trusted store. The device does not need to request the authorization code from the CSSM again and you can enable the feature.

The software features available on Cisco Catalyst IE3x00 Rugged and IE3400H switches fall under these base or add-on license levels.

Base Licenses

- Network Essentials

- Network Advantage—Includes features available with the Network Essentials license and more.

Add-On Licenses

Add-On Licenses require a Network Essentials or Network Advantage as a pre-requisite. The features available with add-on license levels provide Cisco innovations on the switch, as well as on the Cisco Digital Network Architecture Center (Cisco DNA Center).

- DNA Essentials

- DNA Advantage— Includes features available with the DNA Essentials license and more.

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

Feature Licenses

Feature Licenses are bound to a specific feature or set of features. Feature licenses can be enabled regardless of Base License (Network Advantage or Network Essential). Feature licenses are Smart Licenses as well and require a Smart Account to be activated.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

65

Note The MRP feature license requirement is removed in Cisco IOS XE 17.7.1 and later. The MRP feature is available as a part of Network Essentials Licensing. In releases prior to Cisco IOS XE 17.7.1, use of MRP requires a feature license and the following information applies only to those earlier releases.

There are 2 MRP licenses available for IE3x00:

- LIC-MRP-MGR-XE= MRP Ring Manager license.

- LIC-MRP-CLIENT-XE= MRP Ring Client license.

See Activating the MRP License, on page 69 for procedures to activate the MRP license.

For more information about Smart Licensing, see Smart Licensing Using Policy for Cisco Enterprise Routing Platforms.

Multiple MRP Rings

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

Note The MRP feature license requirement is removed in Cisco IOS XE 17.7.1 and later.

You can configure up to three rings, and you can configure the switch as either automanager or client.

MRP-STP Interoperability

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

MRP-STP interoperability is supported for both PROFINET MRP mode and MRP CLI mode, and functions without additional CLI configuration.

Prerequisites

- Before configuring a ring, in Cisco IOS XE releases 17.6.x and earlier, ensure that you have enabled MRP Manager/Client licenses. These can be obtained from Smart licensing account, and by following the SL or SLR process to activate the feature licenses.

- Use of MRP in Cisco IOS XE 17.7.1 and later is available with the Networking Essentials license.

- Because MRP is deployed in a physical Ring topology, before configuring or unconfiguring the MRP feature, it is advised to leave one physical connection between two nodes in each ring open by either issuing a **shut** command on the connecting interfaces or physically removing the cable to avoid any

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

66

network storms. After you have properly configured all MRCs and MRMs, issue a **no shut** command on the port or re-connect the cable between the nodes.

- In Cisco IOS XE releases 17.6.x and earlier, activate the MRP License before you configure the MRP protocol.

- Determine the MRP configuration on the switch: MRA, or MRC.

- When the network is managed by SIMATIC TIA or STEP7, ensure that the basic PROFINET connection is on.

- The MRP default VLAN is 1. To use a non-default VLAN, you must configure the PROFINET VLAN ID before assigning it to the MRP configuration.

Guidelines and Limitations

- MRP is supported on Cisco Catalyst IE3x00 and IE3100 Rugged Series and IE3400 Heavy Duty Series Switches. MRP is not supported on ESS3300 Switches.

- In Cisco IOS XE 17.7.1 and later, the MRP feature is available as a part of Network Essentials Licensing. In releases prior to Cisco IOS XE 17.7.1, use of MRP requires a feature license that must be activated using the Cisco switch CLI.

- By default, Profinet MRP mode is enabled on Cisco Catalyst IE3x00 switches. You can configure MRP, including the MRP role, using the Cisco switch CLI only after you disable the PROFINET MRP function using the Cisco switch CLI.

> ✎
>
> **Note**   Profinet MRP mode is not supported by default on Cisco Catalyst IE3x00 switches. You must use the Cisco switch CLI for configuration.

When PROFINET MRP is enabled, use STEP7 and TIA to configure MRP, including the MRP role.

- To avoid Smart License registration failure, ensure that the NTP configuration and the device clock are in sync.

- With the MRP manager license (Cisco IOS XE 17.6.x and earlier), you can configure up to three rings on a device (each MRP instance can be manager or client), with a manager instance for each ring.

- Support for multiple MRP rings is available only through the CLI or WebUI.

- The switch supports up to 50 MRCs per ring.

- MRP cannot run on the same interface (port) as Resilient Ethernet Protocol (REP), Spanning Tree Protocol (STP), Flex Links, macsec, or Dot1x.

- STP does not run on MRP segments. MRP interfaces drop all STP BPDUs.

- For access ports, you must specifically configure **switchport mode access** and **switchport access vlan** *x* commands in the MRP interface.

- MRP interfaces come up in a forwarding state and remain in a forwarding state until notified that it is safe to block. The MRP ring state changes to Ring-Closed.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

67

- MRP ports cannot be configured as any of these port types: SPAN destination port, Private VLAN port, or Tunnel port. Additionally, when operating in PROFINET mode, you cannot configure MRP ports as Trunk ports.

- MRP is not supported on EtherChannels or on an individual port that belongs to an EtherChannel.

- Each MRP ring can have one MRP VLAN. The VLAN must be different for each ring in a device to avoid traffic flooding.

PROFINET MRP Mode Only

- PROFINET MRP mode is supported on IE3x00 Series Switches; it is not supported on IE3100 Rugged Series Switches.

- Ensure that you configure the correct ring ID on client and manager. Ring ID configuration is not automatically validated by the switch.

- You can configure only one MRP ring in PROFINET MRP mode.

Note The number of MRP rings displayed in the **show profinet status** command output indicates the maximum number of rings allowed for configuration through the CLI and not through PROFINET.

- In PROFINET MRP, which is managed by STEP7 and TIA, only Layer 2 access ports are supported because PROFINET does not have the concept of VLAN tagging.

- The 10 ms profile is not supported.

- When using PROFINET MRP mode, we recommend setting the LLDP timer to 5 ms or 10 ms to ensure PROFINET can see neighbor devices and to avoid a Siemens PLC timeout.

- When a new pluggable module GSD file is installed in TIA/ STEP7, you must recreate the project in TIA/Step7. The existing project, which was created using the old GSD file, will display an error when you attempt to select the new GSD file for the same device. This occurs because the combo ports in the pluggable module SKUs were previously defined as fixed ports.

- You cannot change the role of any node from MRA to MRC after all nodes come up in MRA mode, either by breaking the ring (by shutting the port or physically removing the cable) or manually configuring the role change. If you want an MRP ring configuration with MRA and MRCs, you need to initially configure only one node as MRA and the rest as MRCs.

MRP CLI Mode Only

- After using the CLI to configure the MRP ring, you must attach the MRP ring to a pair of ports that support MRP.

- Both MRP ports must have the same interface mode (access or trunk).

- To change an existing MRP ring's configuration (mode), or to change the interface mode of the ring ports between access and trunk, you must first delete the ring and then recreate it with the new configuration.

- When both MRP ports are in access mode, the access VLANs should match. If the configured MRP VLAN does not match the ports' access VLAN, the MRP VLAN is automatically changed to the MRP ports' access VLAN.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

68

• In an MRP ring with two access ports, if the ports do not belong to the same access VLAN when you create the MRP ring or you change the access VLAN for only one of the ports after the MRP ring is created, the MRP ring operation is suspended and a message similar to the following is displayed:

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

Resolve the issue by configuring the access VLAN to be the same for the two ring ports.

• The 200 ms standard profile, 500 ms profile, and 30 ms profile are supported. The 10 ms profile is not supported.

• MRA can be activated through CLI and PROFINET.

Default Settings

• In Cisco IOS XE 17.6.x and earlier, MRM and MRC licenses are not installed by default. Starting with 17.7.1 a feature license is no longer required for MRP.

• (Cisco IOS XE 17.6.x and earlier) PROFINET MRP mode is enabled by default when MRM or MRC licenses are enabled.

• MRP is disabled by default.

• The default VLAN is 1.

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

Activating the MRP License

Note   Activating the MRP license applies to Cisco IOS XE 17.6.x and earlier. The MRP feature license requirement is removed in Cisco IOS XE 17.7.1 and later.

The procedure to activate the MRP license depends on whether you are using Smart Licensing in online mode or offline mode. Each mode has two scenarios:

• Online mode:

  • The device is connected directly to the Cisco Smart Software Manager (CSSM).

  • The device is connected to the CSSM through the CSLU.

• Offine mode:

  • The device is not connected to the CSSM or the CSLU.

  • The device is in CSLU mode and not connected to the CSSM.

Perform one of the following procedures to activate the MRP license, based on your Smart Licensing mode.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

69

✎

| Note | The following procedures show examples of activating both the MRP Manager and Client licenses. When activating the MRP license on your switch, enter the commands for your license type: mrp-manager or mrp-client. |

Device Directly Connected to CSSM

To activate the MRP license when the device is directly connected to the CSSM, follow these steps.

Step 1   Enter configuration mode:

configure terminal

Step 2   Configure the transport mode:

license smart transport smart

license smart url smart *<url>*

Example:

```
conf t
(config)#license smart transport smart
(config)# license smart url smart https://smartreceiver.cisco.com/licservice/license
(config)#end
wr
```

Step 3   Check the transport mode configuration:

show license all

Example:

```
Switch#show license all
Transport:
  Type: Smart
  URL: license smart url smart https://smartreceiver.cisco.com/licservice/license
```

Step 4   Establish trust with the CSSM:

license smart trust idtoken *<idtoken>* **local force**

A syslog message indicates if trust is established.

Step 5   Verify that trust got established:

show license tech sup | i INSTALL

Example:

```
Switch#show licence tech sup | i INSTALL
      Reservation status: NOT INSTALLED
Local Device: P:IE-3300-8T2X,S:FCW24160H8C, state[2], Trust Data INSTALLED
Overall Trust: INSTALLED (2)
Switch#
```

Step 6   Request and install the Smart License Authorization Code (SLAC) to allow usage of MRP licenses:

license smart authorization request add mrp_manager local

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

70

or

license smart authorization request add mrp_client local

Example:

```
Switch#license smart authorization request add mrp_manager local
Switch#license smart authorization request add mrp_client local
Switch#show licence summary

License Usage:

  License                 Entitlement tag            Count Status

  --------------------------------------------------------------------------

  network-advantage       (IE3400H_Network_Advantage)    1 IN USE

  dna-essentials          (IE3400H_DNA_Essentials)       1 IN USE

  MRP ring manager lic... (IE3x00_LIC_MRP_Manager)       0 NOT IN USE

  MRP ring client lice... (IE3x00_LIC_MRP_Client)        0 NOT IN USE

Switch #
```

Step 7 Enable the MRP feature:

platform license feature mrp-manager

or

platform license feature mrp-client

Example:

```
Switch(config)#platform license feature mrp-manager
Switch(config)#platform license feature mrp-client
Switch#show license summary
License Usage:
  License                 Entitlement tag            Count Status
  --------------------------------------------------------------------------
  network-advantage       (IE3400H_Network_Advantage)    1 IN USE
  dna-essentials          (IE3400H_DNA_Essentials)       1 IN USE
  mrp_manager             (IE3x00_LIC_MRP_Manager)       1 IN USE
  mrp_client              (IE3x00_LIC_MRP_Client)        1 IN USE
```

Device Connected to CSSM through CSLU

To activate the MRP license when the device is connected to the CSSM through the CLSU, follow these steps.

Step 1 Enter configuration mode:

configure terminal

Step 2 Configure the transport mode:

license smart transport cslu

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

71

license smart url cslu http://*<ip-of-windows-machine>***:8182/cslu/v1/pi**

Example:

```
Switch#conf t
Switch(config)#license smart transport cslu
Switch(config)#license smart url cslu http://10.65.77.61:8182/cslu/v1/pi

Switch(config)#end

wr
```

Step 3   Check the transport mode configuration:

show license all

Example:

```
Switch#show license all
Transport:
  Type: cslu
  Cslu address: http://10.65.77.61:8182/cslu/v1/pi
```

Step 4   In the CSLU, enter the required information such as the CSSM URL, Smart Account, and Virtual Account, as shown below, and log in to the CSSM.

Step 5   Request and install the Smart License Authorization Code (SLAC) to allow usage of MRP licenses:

license smart authorization request add mrp_manager local

or

license smart authorization request add mrp_client local

Example:

```
Switch#license smart authorization request add mrp_manager local
Switch#license smart authorization request add mrp_client local
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

72

```
Switch#show licence summary

License Usage:

  License                  Entitlement tag              Count Status

  --------------------------------------------------------------------------

  network-advantage    (IE3400H_Network_Advantage)      1 IN USE

  dna-essentials       (IE3400H_DNA_Essentials)         1 IN USE

  MRP ring manager lic... (IE3x00_LIC_MRP_Manager)      0 NOT IN USE

  MRP ring client lice... (IE3x00_LIC_MRP_Client)       0 NOT IN USE

Switch #
```

Step 6   Enable the MRP feature:

platform license feature mrp-manager

or

platform license feature mrp-client

Example:

```
Switch(config)#platform license feature mrp-manager
Switch(config)#platform license feature mrp-client
Switch#show license summary
License Usage:
  License                  Entitlement tag              Count Status
  --------------------------------------------------------------------------
  network-advantage    (IE3400H_Network_Advantage)      1 IN USE
  dna-essentials       (IE3400H_DNA_Essentials)         1 IN USE
  mrp_manager          (IE3x00_LIC_MRP_Manager)         1 IN USE
  mrp_client           (IE3x00_LIC_MRP_Client)          1 IN USE
```

Device Not Connected to CSSM or CSLU

To activate the MRP license when the device is not connected to the CSSM or the CSLU, follow these steps.

Step 1   Configure the transport mode:

license smart transport off

Example:

```
conf t
(config)#license smart transport off
```

Step 2   Check the transport mode configuration:

show license all

Example:

```
Switch#show license all
Transport:
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches ■

73

```
Type: Transport Off
```

Step 3 To download the Authorization code, go to CSSM > Product Instances, click on **Authorize License-Enforced Features**, and follow the steps.

a) Enter the device identifiers:

b) Enter the required number of MRP licenses:

c) Select the device type:

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

74

d) Verify device and licenses:
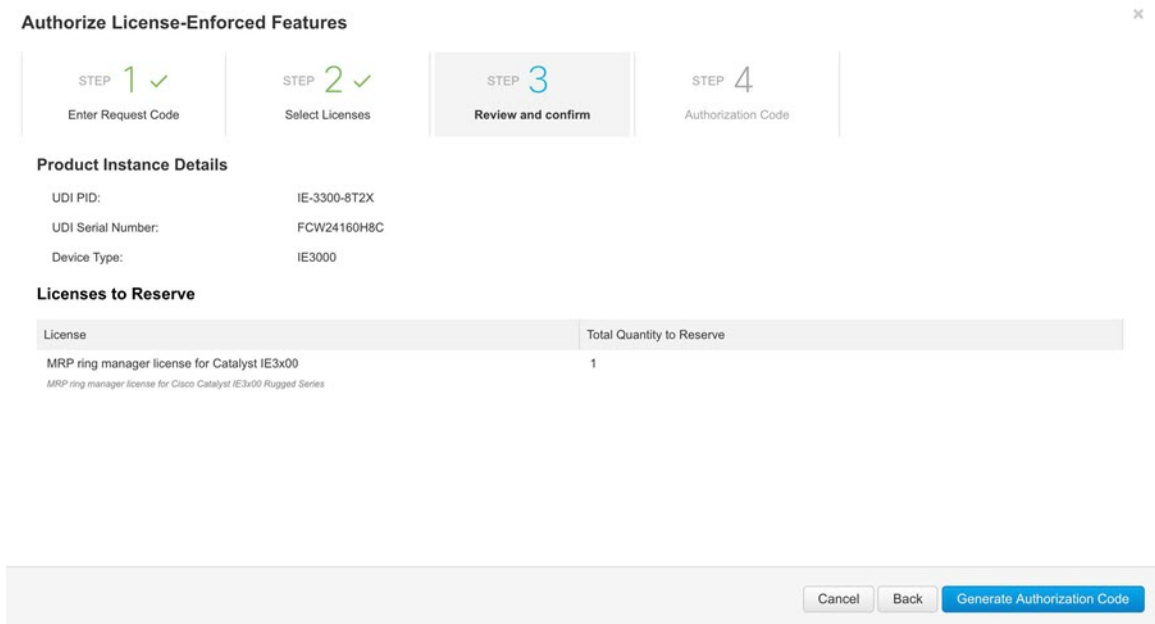
e) Click **Download as File** or **Copy to Clipboard** to obtain the Authorization Code:

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches ■

75

Authorize License-Enforced Features

STEP 1 ✓	STEP 2 ✓	STEP 3 ✓	STEP 4
Enter Request Code	Select Licenses	Review and confirm	Authorization Code

✓ The Reservation Authorization Code below has been generated for this product instance.
Enter this code into the Smart Licensing settings for the product, to enable the licensed features.

Product Instance Details

UDI PID: IE-3300-8T2X

UDI Serial Number: FCW24160H8C

Authorization Code:

```
<smartLicenseAuthorization><udi>P:IE-3300-8T2X,S:FCW24160H8C</udi><authorizationCode><customerInfo><smartAccount>BU Production Test</smartAccount><virtualAccount>Petra-Hellcat
Testing</virtualAccount></customerInfo><flag>A</flag><version>C</version><piid>7f850c96-bfce-48d6-a872-2fbdf44fa02b</piid><dateStamp>2020-11-20T05:23:58</dateStamp><entitlements>
<entitlement><tag>regid.2019-02.com.cisco.IE3x00_LIC_MRP_Manager,1.0_af7ba576-36e3-49a6-ac8b-ddc51e3591fa</tag><count>1</count><startDate></startDate><endDate></endDate>
<licenseType>PERPETUAL</licenseType><displayName>MRP ring manager license for Catalyst IE3x00</displayName><tagDescription>MRP ring manager license for Cisco Catalyst IE3x00
Rugged Series</tagDescription><tagType>PERPETUAL</tagType></entitlement></entitlements></authorizationCode>
<signature>MEUCICvGAh+HMfs1ihwivSt0MxmbZ22+6zDnLDBeDoRHFpxPAiEAgVo//+kmYig4comxY36V+2s/UBE0M7UIrJwKmBQtVjw=</signature></smartLicenseAuthorization>
```

To learn how to enter this code, see the configuration guide for the product being licensed

Download as File   Copy to Clipboard   Close

Step 4   Install the Authorization Code obtained in the previous step in the device:

license smart import *<AuthorizationCode.txt>*

Example:

```
Switch#license smart import AuthorizationCode.txt
Import Data Successfull
Last Confirmation code UDI: PID:IE-3400H-24T,SN:FCW23200H5S
    Confirmation code: 8c55e536
Switch#
```

Step 5   Enable the MRP feature:

platform license feature mrp-manager

or

platform license feature mrp-client

Example:

```
Switch(config)#platform license feature mrp-manager
Switch(config)#platform license feature mrp-client
Switch#show license summary
License Usage:
  License                Entitlement tag               Count Status
  -----------------------------------------------------------------------
  network-advantage      (IE3400H_Network_Advantage)     1 IN USE
  dna-essentials         (IE3400H_DNA_Essentials)        1 IN USE
  mrp_manager            (IE3x00_LIC_MRP_Manager)        1 IN USE
  mrp_client             (IE3x00_LIC_MRP_Client)         1 IN USE
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

76

Device in CSLU Mode and Not Connected to CSSM

To activate the MRP license when the device is in CLSU mode and not connected to the CSSM, follow these steps.

Step 1 Enter configuration mode:

configure terminal

Step 2 Configure the transport mode:

license smart transport cslu

license smart url cslu http://<*ip-of-windows-machine*>**:8182/cslu/v1/pi**

Example:

```
Switch#conf t
Switch(config)#license smart transport cslu
Switch(config)#license smart url cslu http://10.65.77.61:8182/cslu/v1/pi

Switch(config)#end

wr
```

Step 3 Check the transport mode configuration:

show license all

Example:

```
Switch#show license all
Transport:
  Type: cslu
  Cslu address: http://10.65.77.61:8182/cslu/v1/pi
```

Step 4 Send the authorization request from the device to the CLSU.

Export the request to a file on the CSLU, upload the file in CSSM, and get the authorization code from the CSSM.

Step 5 Import the authorization code on the CSLU.

The device will get the authorization code on the next communication with the CSLU and install it.

Step 6 Enable the MRP feature:

platform license feature mrp-manager

or

platform license feature mrp-client

Example:

```
Switch(config)#platform license feature mrp-manager
Switch(config)#platform license feature mrp-client
Switch#show license summary
License Usage:
  License                Entitlement tag              Count Status
  ----------------------------------------------------------------------
  network-advantage      (IE3400H_Network_Advantage)      1 IN USE
  dna-essentials         (IE3400H_DNA_Essentials)         1 IN USE
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

77

```
mrp_manager            (IE3x00_LIC_MRP_Manager)        1 IN USE
mrp_client             (IE3x00_LIC_MRP_Client)         1 IN USE
```

Configuring PROFINET MRP Mode Using TIA 15 or STEP7

After activating the license (Cisco IOS XE 17.6.x and earlier), you can push PROFINET MRP configuration to the Cisco switch using Siemens TIA or STEP7. With IOS XE versions 17.6.x and earlier, the MRP feature license must be installed prior to PROFINET configuring MRP. Starting with IOS XE 17.7.1, MRP can be configured by PROFINET without a feature license.

Note **Do not** use the CLI to configure or modify the switch configuration when PROFINET and TIA are in use. This includes setting the MRC or MRM role. MRP CLI mode and PROFINET MRP modes are mutually exclusive.

Note If the Cisco switch is connected to the PROFINET PLC, the output of **show profinet status | include Connected** is **Yes**. If the output of **show profinet status | include Connected** is **No,** then the switch is not connected to the PROFINET PLC.

Installing the PROFINET GSD File

The PROFINET MRP GSD file is bundled with the Cisco IOS XE software release. After the IE3x00 boots at least one time, the GSD files for the IE3x00 are located in a directory called "ProfinetGSD". In this directory, there is a zip file containing all the GSDs for all IE3x00 SKUs. The file is called "CISCO_Petra_3400.zip. Cisco recommends using the GSD file bundled with the release and included in the ProfinetGSD directory.

Caution If you have a GSD XML file installed in TIA 15 or STEP 7 that is older than the version bundled with the Cisco IOS software, we recommend that you remove the older file to prevent any possible incompatibilities.

Bringing Up PROFINET MRP

Prerequisites

We recommend allowing a MRP Ethernet port, disconnected from the ring (open ring), to discover all the neighbor devices using the LLDP protocol, before pushing the PROFINET MRP to the network. This approach avoids any unnecessary flooding should there be any issues.

SUMMARY STEPS

1. (Optional) Verify that the LLDP protocol discovers all neighbors correctly by entering **show lldp neighbor**.
2. (Cisco IOS XE 17.6 and earlier) Verify that all of the MRP licenses are active on the switch.
3. Ensure PROFINET status shows as connected.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

78

    4. Inspect the output of **profinet mrp ring 1** to confirm that the MRP ports connected correctly and report:

DETAILED STEPS

Step 1   (Optional) Verify that the LLDP protocol discovers all neighbors correctly by entering **show lldp neighbor**.

Step 2   (Cisco IOS XE 17.6 and earlier) Verify that all of the MRP licenses are active on the switch.

Step 3   Ensure PROFINET status shows as connected.

Step 4   Inspect the output of **profinet mrp ring 1** to confirm that the MRP ports connected correctly and report:

- One MRM port in blocked mode

- All other (balance of) MRM ports in forwarding mode

Note   Before making a MRP device role change (such as MRP client to MRP manager or MRP manager to MRP client), make sure that the MRP ring is OPEN.

Managing PROFINET Using Simatic Step 7 or TIA 15 Portal

This section provides an overview of key screens within the TIA portal. It does not provide any configuration details. For details on using the TIA portal, refer to the Siemens Simatic STEP7 user documentation.

Note   MRP automanager in PROFINET mode is supported only in TIA V15.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

79

Figure 5: PROFINET Device Discovery (DCP) Window Before Configuring MRP

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

80
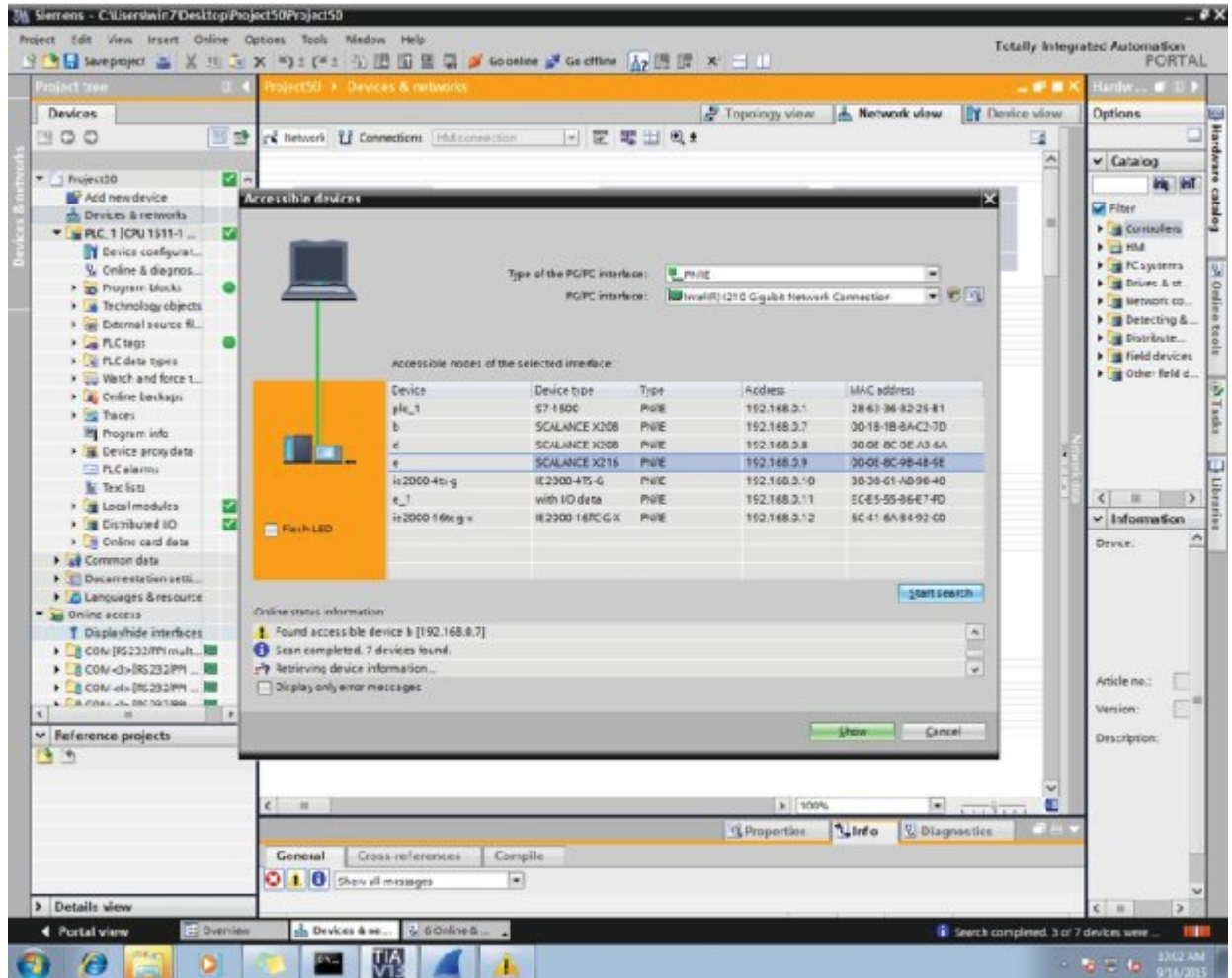
Figure 6: Define PROFINET MRP Manager and MRP domain

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

81
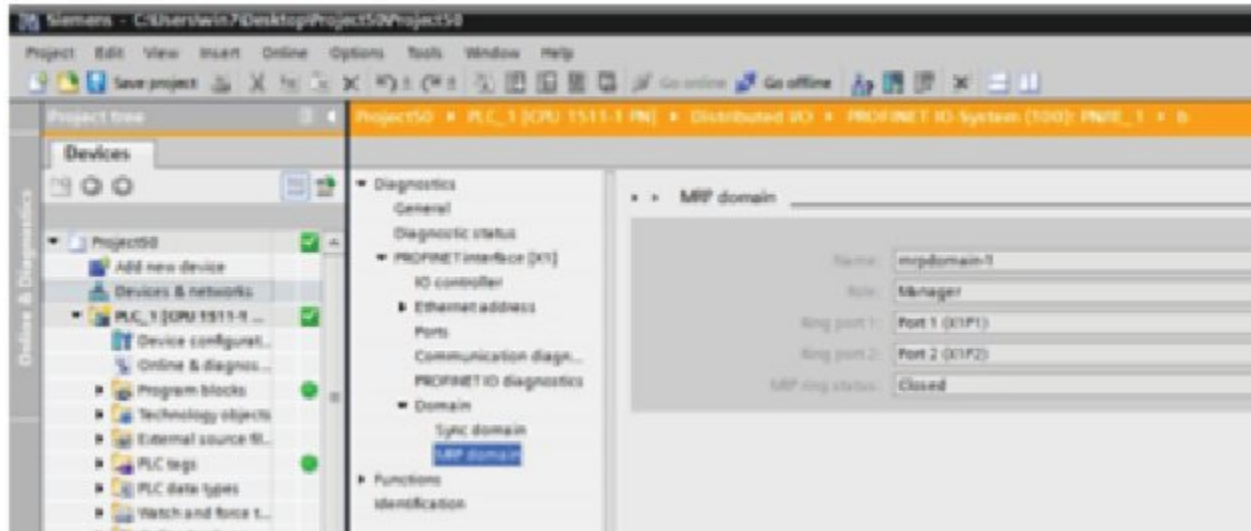
Figure 7: Define PROFINET MRP Client and MRP Domain

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

82
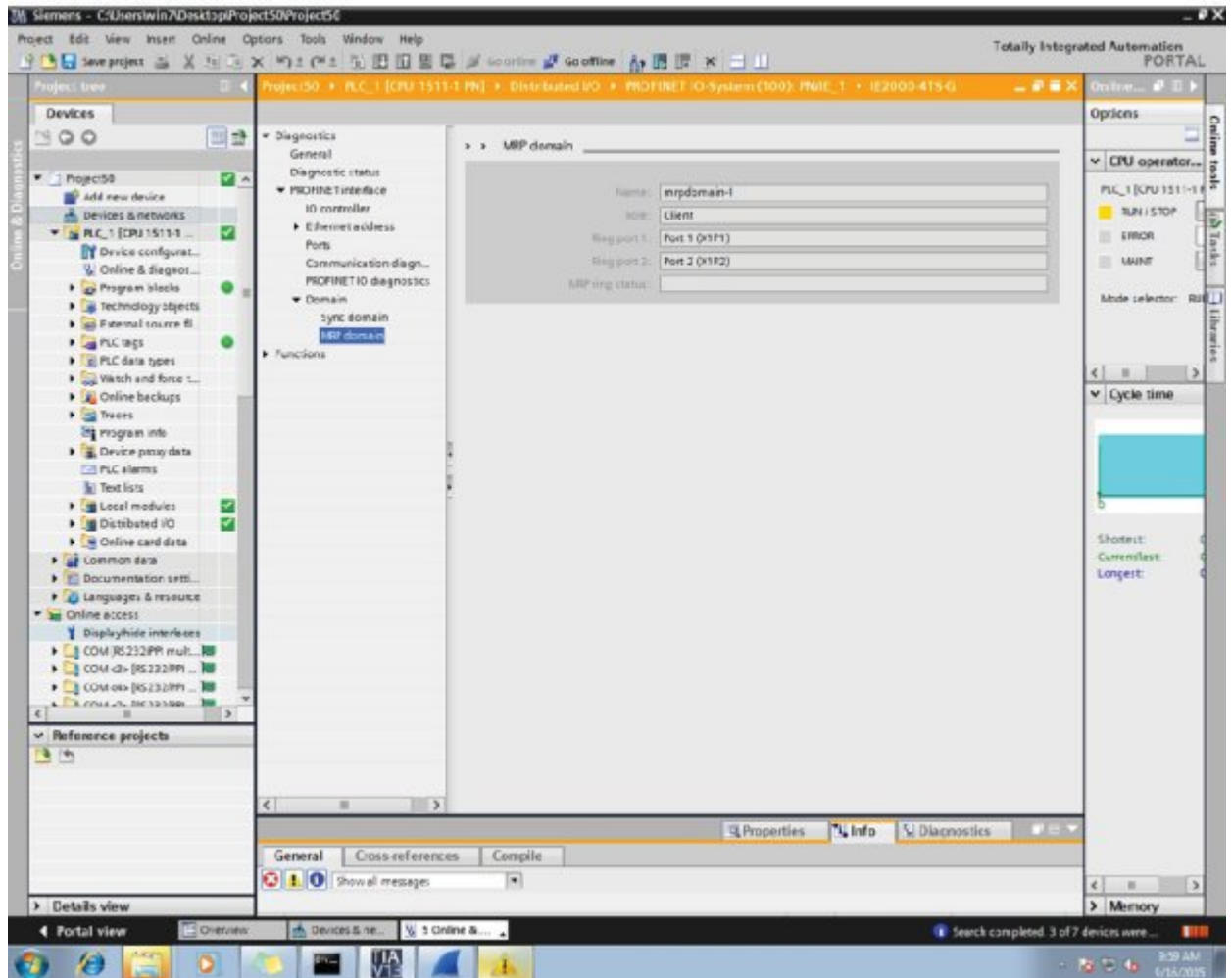
Figure 8: Define PROFINET MRP Interfaces

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches ■

83
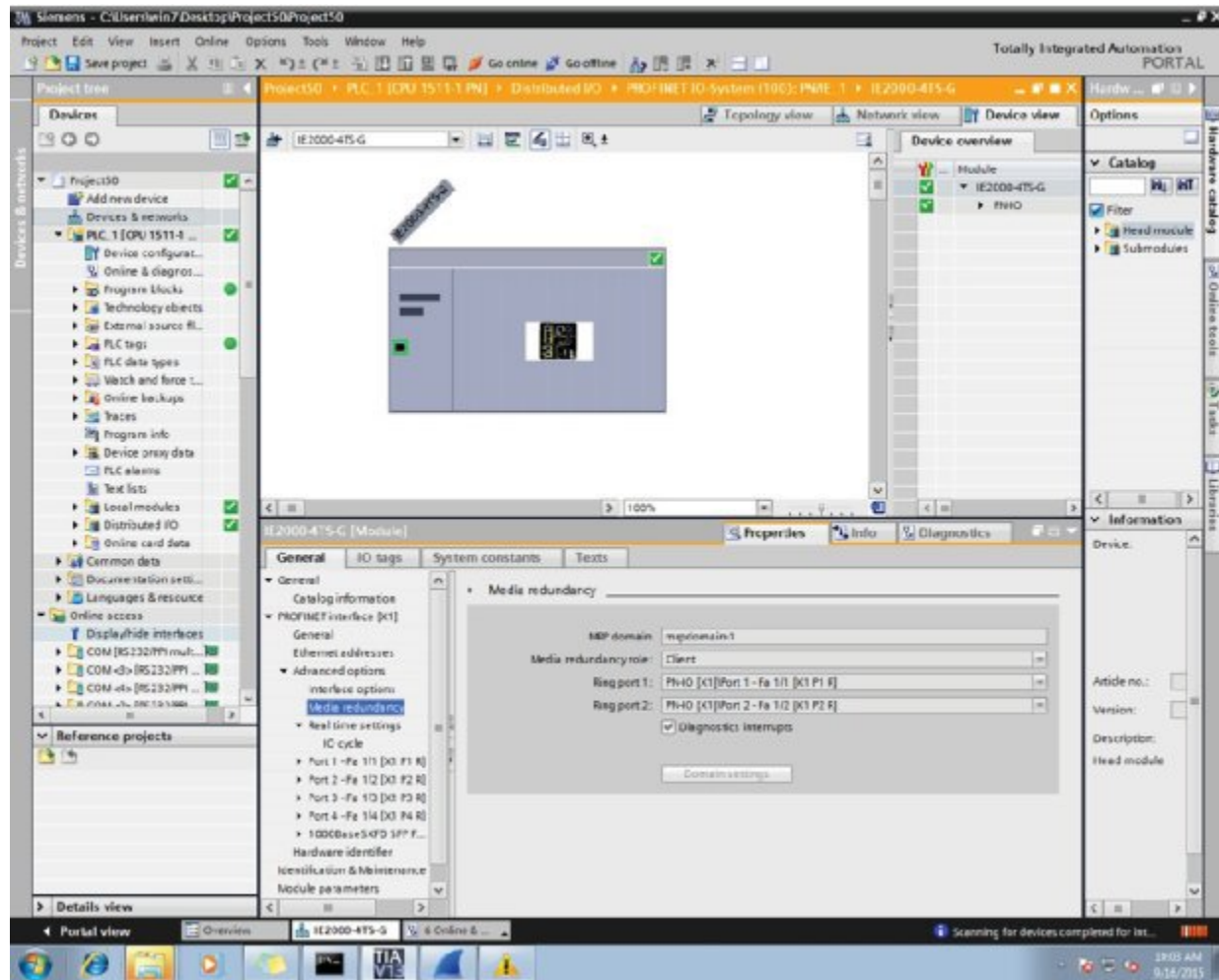
Figure 9: PROFINET MRP Network Configuration Diagram
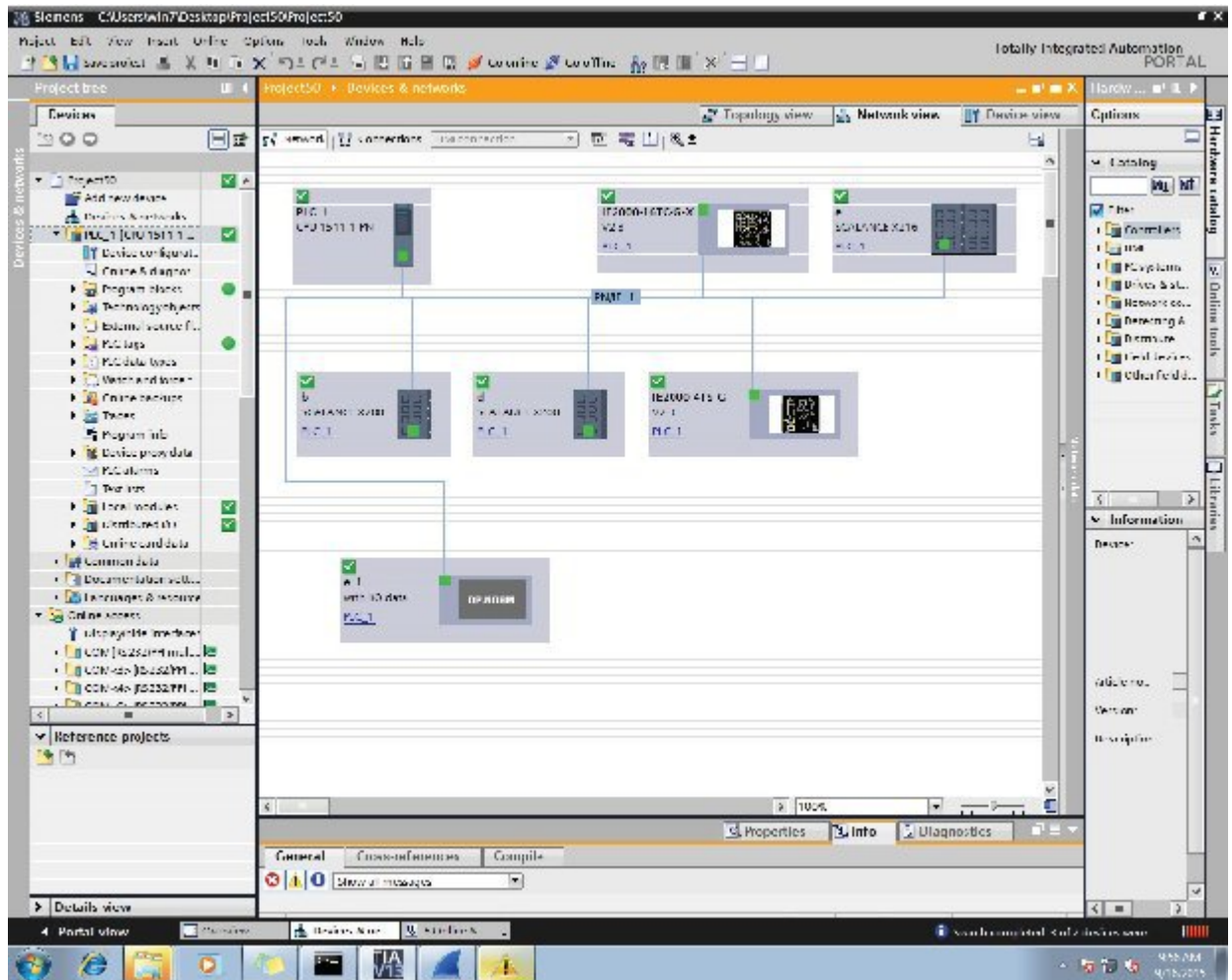
Configuring MRP CLI Mode

To configure MRP, configure the node as MRA or MRC, and specify the two MRP ports. With the mrp-manager license, you can configure up to three rings on the device (the device can be manager or client) with a manager instance for each ring and one manager per device. Each ring with a single MRM can support up to 50 MRCs.

✎

Note The MRP feature license (mrp-manager or mrp-client) applies only to Cisco IOS XE releases earlier than 17.7.1. Use of MRP in Cisco IOS XE 17.7.1 and later does not require a feature license, only the Network Essentials Base license.

The following MRP configuration parameters are optional except for domain-id, which is required for multiple MRP rings, and priority:

• domain-id—A unique ID that represents the MRP ring.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

84

- domain-name—Logical name of the configured MRP domain-ID.

- profile—200 ms (the default)

- vlan-id—VLAN for sending MRP frames.

- default—In global MRP configuration, sets the mode to client.

Configuring MRP Manager

Follow this procedure to configure the switch as MRA in MRP CLI Mode.

Because PROFINET MRP is the default mode of the switch, you will need to disable that mode to allow operation in MRP CLI mode in Step 1 below.

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

SUMMARY STEPS

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

DETAILED STEPS

Step 1   Enter configuration mode:

configure terminal

no profinet mrp

Step 2   Enable MRP:

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

85

mrp ring 1

Step 3 Configure MRP manager mode on the switch:

mode auto-manager

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

domain-id *value*

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

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

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

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

Step 5 (Optional for single MRP ring) Configure the domain name:

domain-name *name*

name —String of up to 32 characters

Step 6 (Optional) Configure the VLAN ID:

vlan-id *vlan*

Step 7 (Optional) Configure the recovery profile:

profile {**30** |**200** | **500**}

- 30—Maximum recovery time 30 milliseconds

- 200—Maximum recovery time 200 milliseconds

- 500—Maximum recovery time 500 milliseconds

Step 8 Configure the MRA priority:

priority *value*

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

The default priority is 40960.

Step 9 Configure the interval:

interval *interval*

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

- 20—20 milliseconds MRP_Test default interval for 200 ms profile

- 50—50 milliseconds MRP_Test default interval for 500 ms profile

- <3-10>—Optional faster MRP_Test interval in milliseconds

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

Step 10 Specify the ID of the port that serves as the first ring port:

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

86

interface *port*

Step 11   Configure the interface mode:

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

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

Step 12   Associate the interface to the MRP ring:

mrp ring 1

Step 13   Return to global configuration mode:

exit

Step 14   Specify the ID of the port that serves as second ring port:

interface *port*

Step 15   Configure the interface mode:

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

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

Step 16   Associate the interface to the MRP ring:

mrp ring 1

Step 17   Return to privileged EXEC mode:

end

Step 18   (For multiple rings) Repeat step 2 through 15 for each additional ring:

 • Assign ring number 2 for the second ring.

 • Assign a unique domain ID for Ring 2. The default domain ID for ring 2 is
   FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFD.

 • Assign ring number 3 for the third ring.

 • Assign a unique domain ID for Ring 3. The default domain ID for ring 3 is
   FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFC.

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

Example

The following example shows configuring MRP automanager:

```
Switch#configure terminal
Switch# no profinet mrp
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#mrp ring 1
Switch(config-mrp)#mode manager
Switch(config-mrp-manager)#domain-id FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

87

```
Switch(config-mrp-manager)#priority 40960
Switch(config-mrp-manager)#end
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#GigabitEthernet1/2
Switch(config-if)#switchport mode trunk
Switch(config-if)#mrp ring 1
WARNING% Enabling MRP automatically set STP FORWARDING. It is recommended to shutdown all
interfaces which are not currently in use to prevent potential bridging loops.
Switch(config-if)#exit
Switch(config)#GigabitEthernet1/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#mrp ring 1
WARNING% Enabling MRP automatically set STP FORWARDING. It is recommended to shutdown all
interfaces which are not currently in use to prevent potential bridging loops.
Switch(config-if)#exit
Switch(config-if)#end

Switch# show mrp ring 1
MRP ring 1

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

Network Topology: Ring
Network Status : OPEN
Port1: Port2:
MAC Address :84:B8:02:ED:E8:02 MAC Address :84:B8:02:ED:E8:01
Interface :GigabitEthernet1/2 Interface :GigabitEthernet1/1
Status :Forwarding Status :Forwarding

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

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

Ring ID : 1
PortName                 Status
------------------------------------
GigabitEthernet1/2       Forwarding
GigabitEthernet1/1       Forwarding
```

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

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

88

Configuring MRP Client

Follow this procedure to configure the switch as an MRP Client.

SUMMARY STEPS

1. Enter configuration mode:

2. Enable MRP:

3. Configure MRP client mode (if you do not specify the mode, client mode is the default):

4. (Optional) Configure the domain ID matching the one configured for this ring on MRM:

5. Return to privileged EXEC mode:

6. Enter configuration mode:

7. Specify the ID of the port that serves as the first ring port:

8. Configure the interface mode:

9. Associate the interface to the MRP ring:

10. Return to global configuration mode:

11. Specify the ID of the port that serves as second ring port:

12. Configure the interface mode:

13. Associate the interface to the MRP ring:

14. Return to privileged EXEC mode:

DETAILED STEPS

Step 1 Enter configuration mode:

configure terminal

Step 2 Enable MRP:

mrp ring 1

Step 3 Configure MRP client mode (if you do not specify the mode, client mode is the default):

mode client

Step 4 (Optional) Configure the domain ID matching the one configured for this ring on MRM:

domain-id *value*

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

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

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

Step 5 Return to privileged EXEC mode:

end

Step 6 Enter configuration mode:

configure terminal

Step 7 Specify the ID of the port that serves as the first ring port:

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

89

interface *port*

Step 8   Configure the interface mode:

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

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

Step 9   Associate the interface to the MRP ring:

mrp ring 1

Step 10   Return to global configuration mode:

exit

Step 11   Specify the ID of the port that serves as second ring port:

interface *port*

Step 12   Configure the interface mode:

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

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

Step 13   Associate the interface to the MRP ring:

mrp ring 1

Step 14   Return to privileged EXEC mode:

end

Example

The following example shows configuring MRP client:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#mrp ring 1
Switch(config-mrp)#mode client
Switch(config-mrp-client)#end
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface gi1/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#mrp ring 1
Switch(config-if)#exit
Switch(config)#interface gi1/2
Switch(config-if)#switchport mode trunk
Switch(config-if)#mrp ring 1
Switch(config-if)#end

Switch#show mrp ring
MRP ring 1

Mode : Client
From : CLI
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

90

```
License : Active
Best Manager :
MAC Address : Unknown
Priority : Unknown

Network Topology: Ring
Network Status : Unknown
Port1: Port2:
MAC Address :30:F7:0D:68:07:81 MAC Address :30:F7:0D:68:07:82
Interface :GigabitEthernet1/1 Interface :GigabitEthernet1/2
Status :Forwarding Status :Forwarding

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

Link Down Timer Interval : 20 ms
Link Up Timer Interval : 20 ms
Link Change (Up or Down) count : 4 ms
MRP ring 2 not configured
MRP ring 3 not configured
```

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

Re-enabling PROFINET MRP

PROFINET MRP is enabled by default. Follow these steps only if your switch is currently operating in MRP CLI mode and you wish to change the operating mode back to PROFINET MRP.

Note Do not configure **switchport mode trunk on** the interfaces that you want to configure for PROFINET MRP. You can have default vlan mode/no configuration or **switchport access vlan 1** CLI configuration on the PROFINET MRP interfaces.

SUMMARY STEPS

1. Enter configuration mode:
2. Enable PROFINET MRP:
3. Configure PROFINET MRP Client or PROFINET MRP Manager using the TIA portal.

DETAILED STEPS

Step 1 Enter configuration mode:

configure terminal

Step 2 Enable PROFINET MRP:

profinet mrp

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

91

Step 3   Configure PROFINET MRP Client or PROFINET MRP Manager using the TIA portal.

The following example shows how to enable PROFINET MRP and check the status:

Example

```
switch#configure terminal
switch(config)# profinet mrp
switch(config)# end
switch#show profinet status
Profinet : Enabled
Connection Status : Connected
Vlan : 50
Profinet ID : ie2km1
GSD version : Match
Reduct Ratio : 128
MRP : Enabled
MRP License Status : Active
MRP Max Rings Allowed : 3
MRC2# sh profinet mrp ring 1
MRP ring 1
Profile     : 200 ms
Mode        : Client
From        : Profinet
Network Topology: Ring
PNPORT 1:(0/32769)    PNPORT 2:(0/32770)
 MAC Address    :78:DA:6E:57:9C:83         MAC Address
:78:DA:6E:57:9C:84
 Interface      :gigabitEthernet1/1         Interface       :gigabitEthernet1/2
 Status         :Forwarding                 Status          :Forwarding
VLAN ID      : 1
Domain Name : mrpdomain-1
Domain ID    : C3D687FE789E3A1ACDBE5BFCBBC27B6
Topology Change Request Interval     : 10ms
Topology Change Repeat Count         : 3
Short Test Frame Interval            : 10ms
Default Test Frame Interval          : 20ms
Test Monitoring Interval Count       : 3
Test Monitoring Extended Interval Count : N/A
```

Verifying Configuration

Command	Description
show mrp ring {1 - 3}	Display details about the MRP ring configuration.
show mrp ports	Display details about the MRP port states. If MRP is not configured on any ports, display shows N/A.
**show mrp ring {1 - 3} statistics [all	event	hardware	packet	platform]**	Display details about the MRP ring operation.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

92

Command	Description
debug mrp [**alarm**|**cli** | **client** | **license** | **manager** | **packet** | **platform**]	Trace MRP events. **Note** **manager** is available only when the switch is configured as manager or automanager. **license** is available only in Cisco IOS XE 17.6.x and earlier.
show profinet status	Display details about PROFINET.
show profinet mrp ring *ring id*	Display details about the PROFINET MRP ring configuration.
show tech-supportprofinet	Display all Profinet details.

Command	Description
show mrp ring {**1 - 3**}	Display details about the MRP ring configuration.
show mrp ports	Display details about the MRP port states. If MRP is not configured on any ports, display shows N/A.
show mrp ring {**1 - 3**} **statistics** [**all** | **event** | **hardware** | **packet** | **platform**]	Display details about the MRP ring operation.
debug mrp-ring [**alarm**|**cli** | **client** | **license** | **manager** | **packet** | **platform**]	Trace MRP events. **Note** **manager** is available only when the switch is configured as manager or automanager. **license** is available only in Cisco IOS XE 17.6.x and earlier.
show profinet status	Display details about PROFINET.
show profinet mrp ring *ring id*	Display details about the PROFINET MRP ring configuration.
show tech-supportprofinet	Display all Profinet details.

Configuration Example

The following example shows the MRP switch configured as manager:

```
Switch#configure terminal
Switch# no profinet mrp
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#mrp ring 1
Switch(config-mrp)#mode manager
Switch(config-mrp-manager)#end
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface gi1/8
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

93

```
Switch(config-if)#switchport mode trunk
Switch(config-if)#mrp ring 1
WARNING% Enabling MRP automatically set STP FORWARDING. It is recommended to shutdown all
interfaces which are not currently in use to prevent potential bridging loops.
Switch(config-if)#exit
Switch(config)#interface gi1/7
Switch(config-if)#switchport mode trunk
Switch(config-if)#mrp ring 1
WARNING% Enabling MRP automatically set STP FORWARDING. It is recommended to shutdown all
interfaces which are not currently in use to prevent potential bridging loops.
Switch(config-if)#end

Switch#show mrp ring
MRP ring 1

Profile     : 200 ms
Mode        : Master
From        : CLI

Network Topology: Ring
Port1:                                  Port2:
MAC Address    :2C:54:2D:2C:3E:0A       MAC Address    :2C:54:2D:2C:3E:09
Interface      :gigabitEthernet1/8      Interface      :gigabitEthernet1/7
Status         :Forwarding              Status         :Forwarding

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

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

Ring ID : 1
PortName                 Status
------------------------------------
gigabitEthernet1/7         Forwarding
gigabitEthernet1/8         Forwarding
```

The following example shows the MRP switch configured as automanager:

```
Switch#configure terminal
Switch# no profinet mrp
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#mrp ring 1
Switch(config-mrp)#mode auto-manager
Switch(config-mrp-auto-manager)#priority 36864
Switch(config-mrp-auto-manager)#end
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface gi1/2
Switch(config-if)#switchport mode trunk
Switch(config-if)#mrp ring 1
WARNING% Enabling MRP automatically set STP FORWARDING. It is recommended to shutdown all
interfaces which are not currently in use to prevent potential bridging loops.
Switch(config-if)#exit
Switch(config)#interface gi1/1
Switch(config-if)#switchport mode trunk
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

94

```
Switch(config-if)#mrp ring 1
WARNING% Enabling MRP automatically set STP FORWARDING. It is recommended to shutdown all
interfaces which are not currently in use to prevent potential bridging loops.
Switch(config-if)#end

Switch#show mrp ring
MRP ring 1

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

Network Topology: Ring
Network Status  : OPEN
Port1:                                  Port2:
 MAC Address    :84:B8:02:ED:E8:02       MAC Address    :84:B8:02:ED:E8:01
 Interface      :GigabitEthernet1/2      Interface      :GigabitEthernet1/1
 Status         :Forwarding              Status         :Forwarding

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

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


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

The following example shows the MRP switch configured as client:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#mrp ring 1
Switch(config-mrp)#mode client
Switch(config-mrp-client)#end
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface gi1/3
Switch(config-if)#switchport mode trunk
Switch(config-if)#mrp ring 1
Switch(config-if)#exit
Switch(config)#interface gi1/4
Switch(config-if)#switchport mode trunk
Switch(config-if)#mrp ring 1
Switch(config-if)#end
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

95

Feature History

The following table shows the Cisco IOS release in which the feature is first supported on each of the IE switch platforms that support MRP.

Switch Platform	Feature	Initial Release
Cisco Catalyst IE3x00 Rugged Series and Cisco Catalyst IE3400 Heavy-Duty Series Switches	MRP Support	Cisco IOS XE Gibraltar 16.12.1
Cisco Catalyst IE3x00 Rugged Series and Cisco Catalyst IE3400 Heavy-Duty Series Switches	MRP-PROFINET	Cisco IOS XE Amsterdam 17.1.1
Cisco Catalyst IE3x00 Rugged Series and Cisco Catalyst IE3400 Heavy-Duty Series Switches	MRP 500ms Profile Support	Cisco IOS XE Amsterdam 17.3.1
Cisco Catalyst IE3x00 Rugged Series and Cisco Catalyst IE3400 Heavy-Duty Series Switches	MRP Support on Trunk Links	Cisco IOS XE Bengaluru 17.4.1
Cisco Catalyst IE3x00 Rugged Series and Cisco Catalyst IE3400 Heavy-Duty Series Switches	MRP License removal	Cisco IOS XE Cupertino 17.7.1
Cisco Catalyst IE3x00 Rugged Series and Cisco Catalyst IE3400 Heavy-Duty Series Switches	MRP: 30ms Profile Support	Cisco IOS XE Cupertino 17.9.1
Cisco Catalyst IE3100 Rugged Series Switches	• MRP: 30ms Profile Support • MRP 200ms Profile Support • MRP 500ms Profile Support • MRP CLI support by default	Cisco IOS XE Dublin 17.11.1

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

96

Configuring PRP

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 only on IE3400 and IE3400H switches running IOS XE. PRP is not supported on the IE3200 and IE3300 series of switches.

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.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

97

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 10: PRP Redundant Network
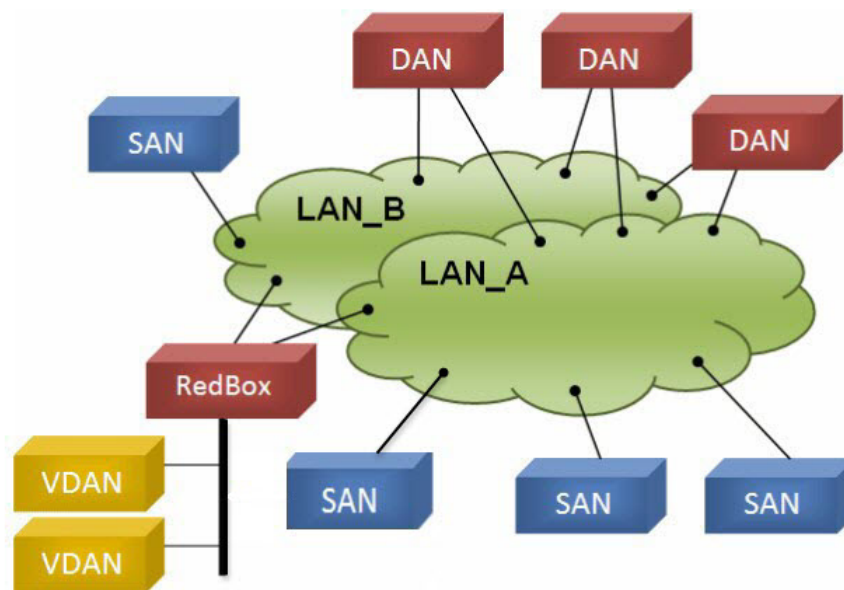
To manage redundancy and check the presence of other DANs, a DAN periodically sends Supervision frames and can evaluate the Supervision frames sent by other DANs.

Role of the Switch

The IE 3400 switch implements RedBox functionality using Gigabit Ethernet port connections to each of the two LANs.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

98

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.

Platform	Channel Group	Ports
IE3400	Channel 1	Gig1/1 (LAN-A) and Gig1/ 2 (LAN-B) or Gig1/3 (LAN-A) and Gig1/4 (LAN-B
	Channel 2	Gig2/1 (LAN-A) and Gig2/2 (LAN-B)
IE3400-H (X-Coded)	Channel 1	Gig1/1 (LAN-A) and Gig1/2 (LAN-B
	Channel 2	Gig1/9 (LAN-A) and Gig1/10 (LAN-B)
IE3400-H (D-Coded)	Channel 1	Fa1/1 (LAN-A) and Fa1/2 (LAN-B)
	Channel 2	Fa1/9 (LAN-A) and Fa1/10 (LAN-B)

Note
- Switch ports that are not part of PRP can function normally and can be used just like any other port.
- PoE Functionality is not affected and works as usual on the PRP-enabled port.

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 Adding Static Entries to the Node and VDAN Tables, on page 119. You can also display the node and VDAN tables and clear entries. See Verifying Configuration, on page 121 and Clearing All Node Table and VDAN Table Dynamic Entries, on page 120.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

99

VLAN Tag in Supervision Frame

Beginning with the Cisco IOS 17.5.1 release, the switch supports 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.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

100
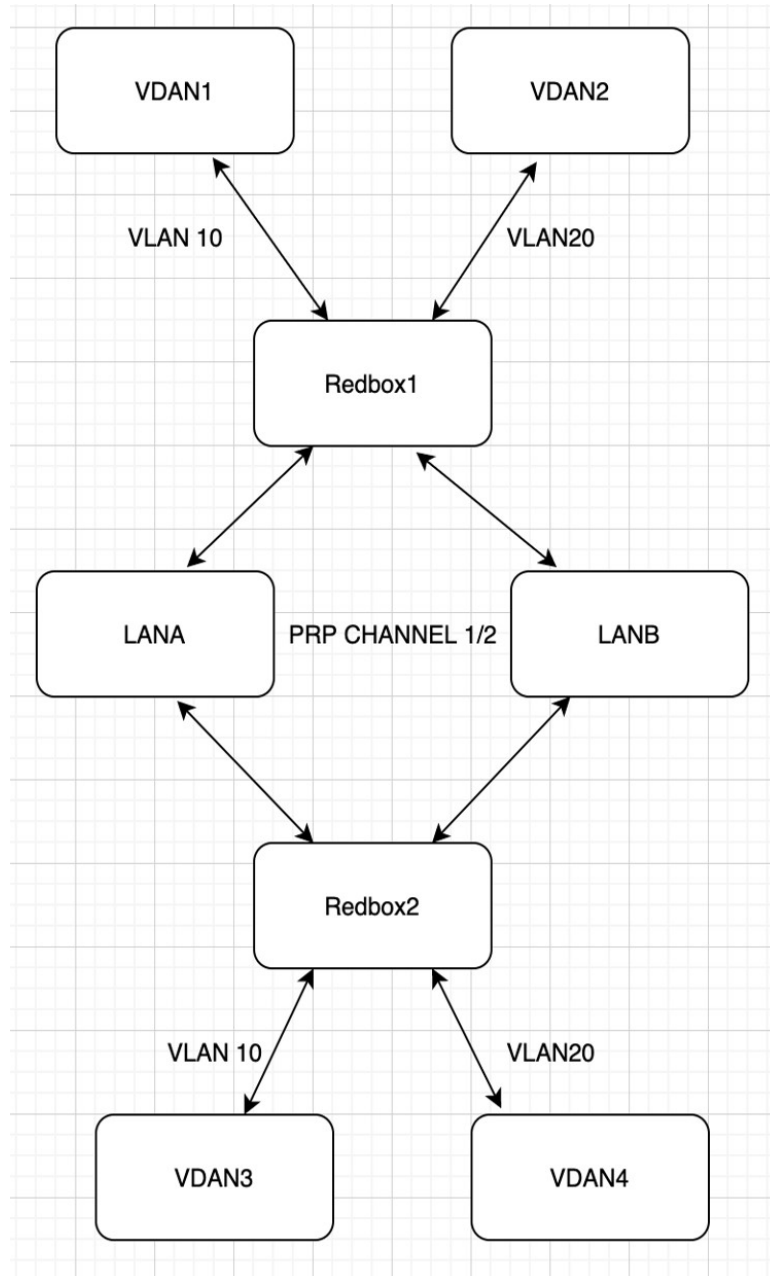
See Configuring PRP Channel with Supervision Frame VLAN Tagging, on page 117 for configuration information.

PTP over PRP

Precision Time Protocol (PTP) can operate over Parallel Redundancy Protocol (PRP). PRP provides high availability through redundancy for PTP. For a description of PTP, see Configuring Precision Time Protocol.

The PRP method of achieving redundancy by parallel transmission over two independent paths (see Information About PRP, on page 97) does not work for PTP as it does for other traffic. The delay experienced by a frame is not the same in the two LANs, and some frames are modified in the transparent clocks (TCs) while transiting through the LAN. A Dually Attached Node (DAN) does not receive the same PTP message from both ports even when the source is the same. Specifically:

- Sync/Follow_Up messages are modified by TCs to adjust the correction field.

- Boundary Clocks (BCs) present in the LAN are not PRP-aware and would generate their own Announce and Sync frames with no Redundancy Control Trailer (RCT) appended.

- Follow_Up frames are generated by every 2-step clock and carry no RCT.

- TCs are not PRP-aware and not obliged to forward the RCT, which is a message part that comes after the payload.

Previously, PTP traffic was allowed only on LAN-A to avoid the issues with PTP and parallel transmission described earlier. However, if LAN-A went down, PTP synchronization was lost. To enable PTP to leverage the benefit of redundancy offered by the underlying PRP infrastructure, PTP packets over PRP networks are handled differently than other types of traffic. The implementation of the PTP over PRP feature is based on the PTP over PRP operation that is detailed in IEC 62439-3:2016, *Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)*. This approach overcomes the problems mentioned earlier by not appending an RCT to PTP packets and bypassing the PRP duplicate/discard logic for PTP packets.

PTP over PRP Packet Flow

The following figure illustrates the operation of PTP over PRP.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

101

Figure 11: PTP over PRP Packet Flow
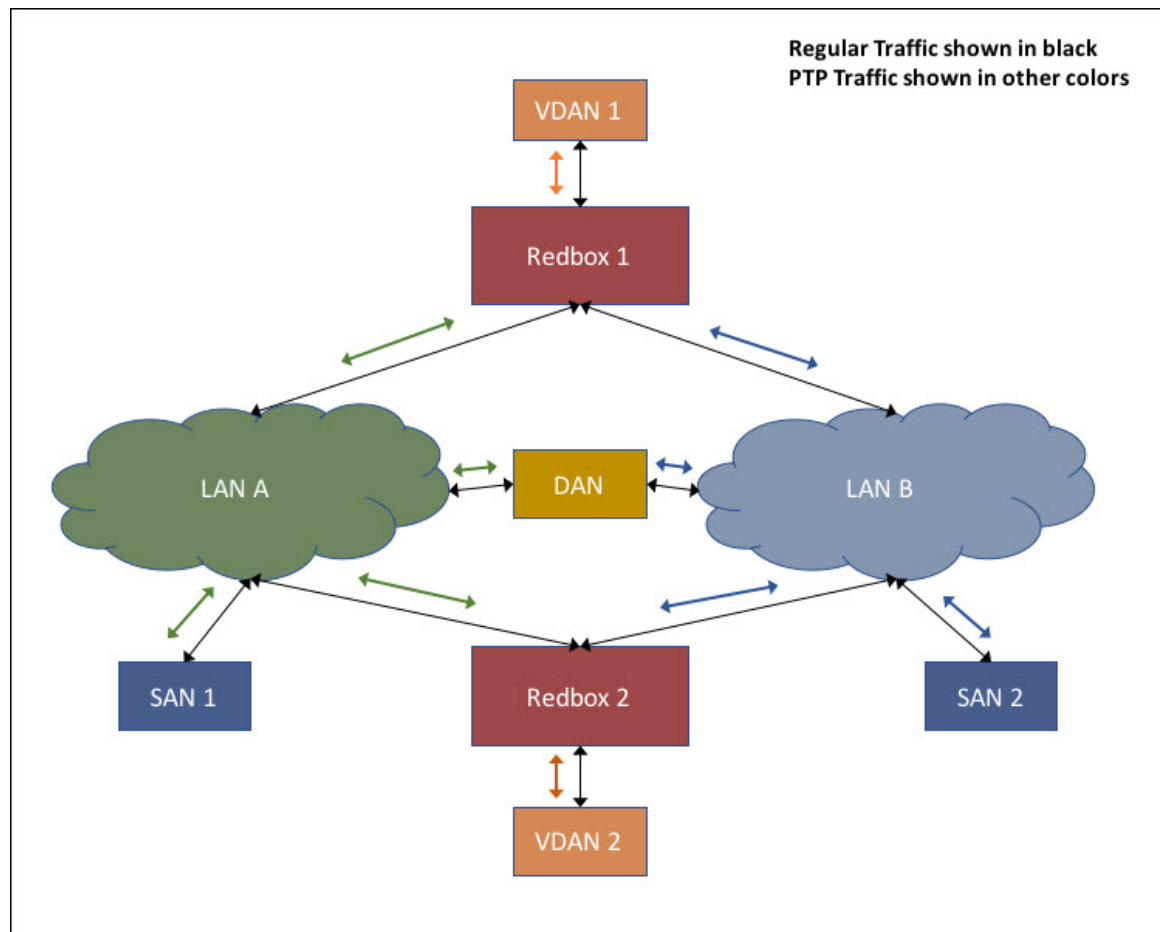
In the figure, VDAN 1 is the grandmaster clock (GMC). Dually attached devices receive PTP synchronization information over both their PRP ports. The LAN-A port and LAN-B port use a different virtual clock that is synchronized to the GMC. However, only one of the ports (referred to as time recipient) is used to synchronize the local clock (VDAN 2 in the figure). While the LAN-A port is the time recipient, the LAN-A port's virtual clock is used to synchronize VDAN-2. The other PRP port, LAN-B, is referred to as PASSIVE. The LAN-B port's virtual clock is still synchronized to the same GMC, but is not used to synchronize VDAN 2.

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

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

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

102

Note   Cisco is moving from the traditional Master/Slave nomenclature. In this document, the terms *Grandmaster clock (GMC)* or *time source* and *time recipient* are used instead.

Supported Location of GMC

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

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

- A VDAN (for example, VDAN 1 in the preceding diagram).

- A DAN (for example, the DAN in the preceding diagram).

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

Configuration

PTP over PRP does not require configuration beyond how you would normally configure PTP and PRP separately, and there is no user interface added for this feature. The difference is that before the PTP over PRP feature, PTP worked over LAN-A only; now it works over both LANs. Before implementing PTP over PRP, refer to Guidelines and Limitations, on page 111.

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

1. Refer to PRP RedBox Types, on page 104 to determine the location of the PRP RedBox. Refer to Configuring Precision Time Protocol to determine PTP mode and profile.

2. Configure PTP as described in Configuring Precision Time Protocol, following the procedure for the PTP profile determined in step 1.

3. Configure PRP as described in Creating a PRP Channel and Group, on page 114.

Supported PTP Profiles and Clock Modes

The following table summarizes PTP over PRP support for the various PTP profiles and clock modes. In unsupported PTP profile/clock mode combinations, PTP traffic flows over LAN-A only. LAN-A is the lower numbered interface. See PRP Channels, on page 99 for PRP interface numbers.

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

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

103

PRP RedBox Types

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

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

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

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

104

Figure 12: PRP Redbox as DABC with E2E
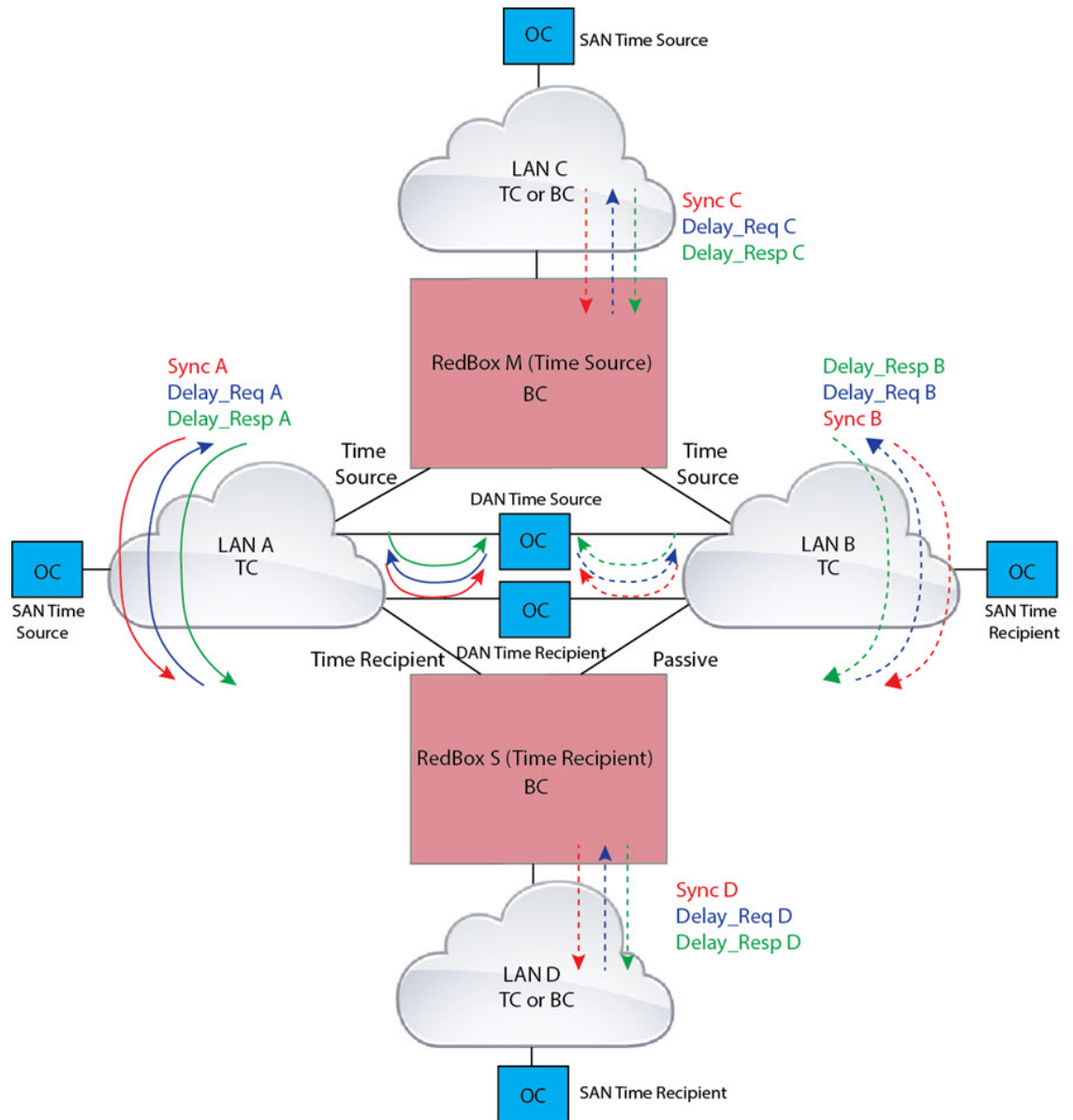
On Redbox S, the regular BMCA operation determines port A to be a time recipient and port B to be PASSIVE. However, with the knowledge that ports A and B are part of the same PRP channel, port B is forced into PASSIVE_SLAVE state. Port A and Port B on Redbox S operate as follows:

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

- Port B is in PASSIVE_SLAVE state. It uses the end-to-end delay measurement mechanism to calculate delay and offset from the time source.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

105

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

PRP RedBox as Doubly Attached BC (DABC) with P2P

The following figure shows an example where Redbox M and Redbox S are configured to run in Power Profile as Boundary Clocks that use Peer-to-Peer (P2P) delay measurement mechanism. In this example, the GMC is the ordinary clock attached through LAN C. All the clocks are configured to run Peer-to-Peer Delay measurement and the peer delay is regularly calculated and maintained on every link shown in the figure.

The BMCA on Redbox M determines ports A and B to be connected to the time source. The PTP protocol running on Redbox M treats both ports A and B individually as time source ports and sends out Sync and Follow_Up messages individually on both the ports.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

106

Figure 13: PRP Redbox as DABC with P2P

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

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

- Port B is in PASSIVE_SLAVE state. Like port A, it maintains the delay and offset from time source, but does not perform any operation on the local clock. Having all the synchronization information available enables it to seamlessly take over as the new time recipient in case port A loses communication with the GM.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

107

PRP RedBox as Doubly Attached TC (DATC) with P2P

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

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

Figure 14: PRP Redbox as DATC with P2P
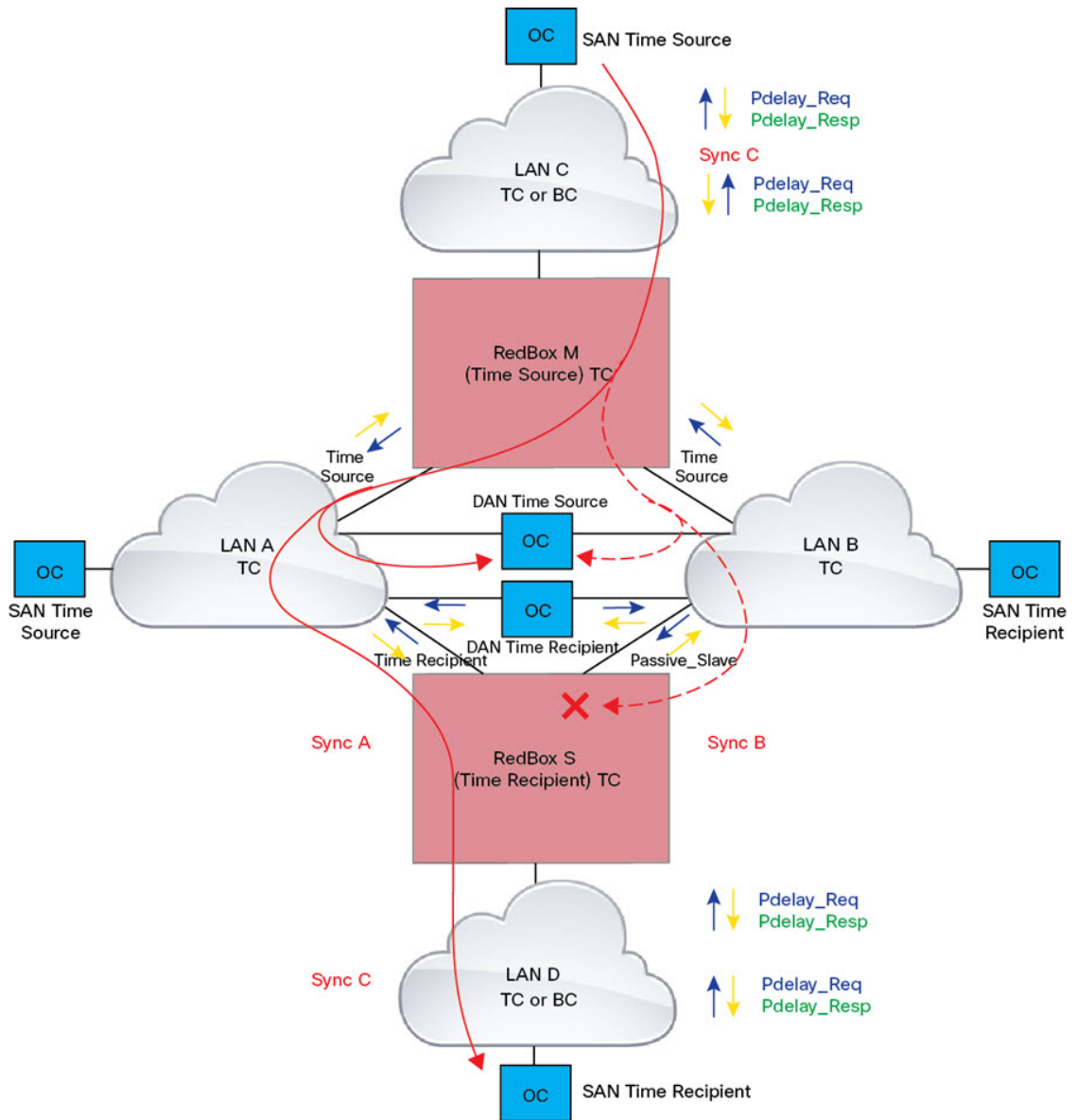
Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

108

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

- Port A works as a regular time recipient port. It uses the Sync and Follow_Up messages along with their correction field to calculate the delay and offset from time source and synchronize the local clock. (Unlike an E2E BC, it does not need to generate Delay_Req messages since all the link delays and residence times along the PTP path are accumulated in the correction field of the Follow_Up messages).

- Like port A, port B maintains the delay and offset from time source, but does not perform any operation on the local clock. Having all the synchronization information available enables it to seamlessly take over as the new time recipient in case port A loses communication with the GMC.

LAN-A and LAN-B Failure Detection and Handling

Failures in LAN-A and LAN-B are detected and handled in the same way for all Redbox types described in PRP RedBox Types, on page 104.

Using the example shown in Figure 14: PRP Redbox as DATC with P2P, on page 108 with the GMC as a SAN in LAN C, a failure in LAN-A or LAN-B pertaining to PTP can occur due to the following reasons:

- A device within the LAN goes down.

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

- PTP messages are dropped within the LAN.

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

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

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

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

TrustSec Configuration on PRP Interface

You can configure TrustSec on member interfaces of a PRP channel. This feature is supported on IE3400 and IE3400H 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, Gi1/1 and Gi1/2. 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.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

109

- 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.

You can configure the PRP channel interfaces using the **interface range <>** command or by configuring each individual interface, as shown in the following examples.

Valid Configuration

This 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 gi1/1
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 gi1/2
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
```

This 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 gi1/1-2
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
```

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 gi1/1
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)#
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

110

Prerequisites

- IE3400 with IEM-3400 (Advanced Expansion Module) or IE3400H

- Network Advantage License

- Cisco IOS XE 17.4 or greater for two PRP channel support

Guidelines and Limitations

- PRP traffic load cannot exceed 90% bandwidth of the Gigabit Ethernet interface channels.

- 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**

    - **system mtu jumbo 1506**

- 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.

- 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 system displays this message:

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

- Load-balancing is not supported.

- UDLD must be disabled on interfaces where PRP is enabled, especially if the interfaces have media-type sfp.

- The **spanning-tree bpdufilter enable** command is required on the prp-channel interface. Spanning-tree BPDU filter drops all ingress/egress BPDU traffic. This command is required to create independent spanning-tree domains (zones) in the network.

- The **spanning-tree portfast edge trunk** command is optional on the prp-channel interface but highly recommended. It improves the spanning-tree converge time in PRP LAN-A and LAN-B.

- The **show interface g1/1** or **show interface g1/2** 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.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches ■

111

- 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 (CSCur88178). IE 5000 output is shown in the following example:

  The following example shows output for the IE5000 series switches:

  ```
  show prp channel detail

  PRP-channel listing:
  --------------------
  PRP-channel: PR1
  ------------
  Layer type = L3
   Ports: 2       Maxports = 2
   Port state = prp-channel is Inuse
   Protocol = Disabled

  Ports in the group:
    1) Port: Gi1/17
     Logical slot/port = 1/17 Port state = Inuse
     Protocol = Enabled
    2) Port: Gi1/18
     Logical slot/port = 1/19 Port state = Inuse
     Protocol = Enabled
  ```

- On IE3400 and IE IE3400H, PRP does not allow member ports in a PRP channel to be shut down. For example, issuing a shut on gi1/3 or gi1/4 when it is part of a PRP channel is not allowed.

  If you attempt to execute **shut** on a PRP member interface, the following message is displayed:

  ```
  switch(config)#int gi 1/3
  switch(config-if)#shut
  %Interface GigabitEthernet1/3 is configured in PRP-channel group, shutdown not permitted!
  ```

- 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: Gi1/3
  Logical slot/port = 1/3 Port state = Inuse
  Protocol = Enabled
  2) Port: Gi1/4
  Logical slot/port = 1/4 Port state = Not-Inuse (link down)
  Protocol = Enabled
  ```

- PRP functionality can be managed using the CIP protocol. The following CIP commands for PRP are available on the IE3400:

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

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

112

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

- The IE3400 does not have a separate PRP/HSR mode LED, unlike the IE4000 that has a PRP/HSR LED on the switch faceplate.

- PRP is not supported on the IE3200 and IE3300 series of switches.

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.

PTP over PRP

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

  No PTP configuration is available under **interface prp-channel**. The PRP channel member interfaces need to be individually configured for PTP. However, in most cases, you do not need to perform any PTP configuration on the interfaces because PTP is enabled by default on all physical Ethernet interfaces.

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

- PTP over PRP can coexist with Device Level Ring (DLR). In this scenario, the PRP RedBox is also part of a DLR network.

- No configuration compatibility is enforced on the PRP channel member interfaces with respect to PTP.

  You can have different PTP configurations on PRP member interfaces. However, we recommend that you have identical PTP configurations on the interfaces that are part of the same PRP channel to allow for seamless transitions between PASSIVE_SLAVE and SLAVE states.

- We recommend that the grandmaster (GM) clock be dually attached to both PRP LANs (as RedBox, VDAN, or DAN). If a GM is singly attached to one of the PRP LANs, only the devices in that LAN will be synchronized to the GM.

- PTP over PRP supports only the Redbox types described in PRP RedBox Types, on page 104. The following Redbox types described in IEC 62439-3, Section A are not supported:

  - PRP RedBoxes as three-port BCs (TWBC) - Section A.4.5.2

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

113

> • PRP RedBox as DATC with E2E - Section A.4.5.4.1
>
> • PRP RedBox as a stateless TC (SLTC) - Section A.4.5.5

- To prevent any switch within PRP LAN-A/B from becoming a Grand Master, when PTP over PRP is configured for the system, other switches in PRP LAN-A and LAN-B should not be configured for PTP boundary mode. PTP transparent mode on PRP LAN-A/B switches is recommended in a time-sensitive environment.

- IE switch platforms do not support PTP profile conversion. For example, if RedBox S in Figure 13: PRP Redbox as DABC with P2P, on page 107 were an IE switch, it would not support Delay_Req/Delay_Resp message exchange with LAN D shown in the figure. It would only support Peer-to-Peer delay measurement mechanism using PDelay messages.

- PTP VLAN behavior remains unchanged by the PTP over PRP feature.

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 99.

Creating 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 99.

- Review the Prerequisites, on page 111 and Guidelines and Limitations, on page 111.

- 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.

The following example is based on the IE3400. Adjust the interface utilized based on the earlier information.

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, non-tagged 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:

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

114

12. Configure bpdufilter on the prp-channel interface:

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

DETAILED STEPS

Step 1   Enter global configuration mode:

configure terminal

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

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, non-tagged 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   Only required 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

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches ■

115

Step 12   Configure bpdufilter on the prp-channel interface:

spanning-tree bpdufilter enable

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

Step 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

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 GigabitEthernet1/1-2
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 with a VLAN ID of 2.

```
switch# configure terminal
switch(config)# interface range GigabitEthernet1/1-2
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 GigabitEthernet1/1-2
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
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

116

```
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 per switch type, described in PRP Channels, on page 99.

- Review the Prerequisites, on page 111 and Guidelines and Limitations, on page 111.

- 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.

The following example is based on the IE3400. Adjust the interface utilized based on the earlier information.

SUMMARY STEPS

1. Enter global configuration mode:
2. Assign two Gigabit Ethernet interfaces to the PRP channel group. For channel 1, enter:
3. Configure the PRP interface for trunk administrative mode, to allow the interface to carry traffic for more than one VLAN.
4. Specify the allowed VLANS for the trunk interface:
5. (Optional) Disable Precision Time Protocol (PTP) on the switch:
6. Disable loop detection for the redundancy channel:
7. Disable UDLD for the redundancy channel:
8. Enter sub-interface mode and create a PRP channel group:
9. Bring up the PRP channel:
10. Specify the PRP interface and enter interface mode:
11. Configure bpdufilter on the prp-channel interface:
12. Set the VLAN ID to be used in VLAN tags for supervision frames:
13. (Optional) Configure the Class of Service (COS) value to be set in the VLAN tag of the Supervision frame:
14. Enable VLAN tagging on the interface:
15. (Optional) Configure LAN-A/B ports to quickly get to FORWARD mode:

DETAILED STEPS

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 {**GigabitEthernet1/1-2** | **GigabitEthernet1/3-4**}

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

117

For channel 2, enter:

interface range {**GigabitEthernet2/1-2** | **GigabitEthernet1/9-10**}

Gi1/9 and Gi 1/10 are supported for IE3400H only. See PRP Channels, on page 99.

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

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

switchport mode trunk

Step 4   Specify the allowed VLANS for the trunk interface:

switchport trunk allowed vlan *value*

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

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

no ptp enable

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

Step 6   Disable loop detection for the redundancy channel:

no keepalive

Step 7   Disable UDLD for the redundancy channel:

udld port disable

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

prp-channel-group *prp-channel group*

prp-channel group—Value of 1 or 2

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

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

Step 9   Bring up the PRP channel:

no shutdown

Step 10   Specify the PRP interface and enter interface mode:

interface prp-channel *prp-channel-number*

prp-channel-number—Value of 1 or 2

Step 11   Configure bpdufilter on the prp-channel interface:

spanning-tree bpdufilter enable

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

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

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

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

118

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 - 7. 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 GigabitEthernet1/1-2
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)# 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
```

Adding Static Entries to the Node and VDAN Tables

Follow this procedure 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 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:

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

119

DETAILED STEPS

Step 1 Enter global configuration mode:

configure terminal

Step 2 Specify the MAC address to add to the node table for the channel group and 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.

Example

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

Clearing All Node Table and VDAN Table Dynamic Entries

To clear all dynamic entries in the node table, enter

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

To clear all dynamic entries in the VDAN table, enter

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** commands shown in .

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

120

Disabling the PRP Channel and Group

SUMMARY STEPS

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

DETAILED STEPS

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

Verifying Configuration

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

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

121

Note The **show interface g1/1** or **show interface g1/2** 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: Gi1/3
Logical slot/port = 1/3 Port state = Inuse
Protocol = Enabled
2) Port: Gi1/4
Logical slot/port = 1/4 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
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

122

```
REDBOX1#
```

Configuration Examples

The following diagram shows a network configuration in which the IE3400 and IE3400H might operate. The commands in this example highlight the configuration of features and switches to support that configuration.
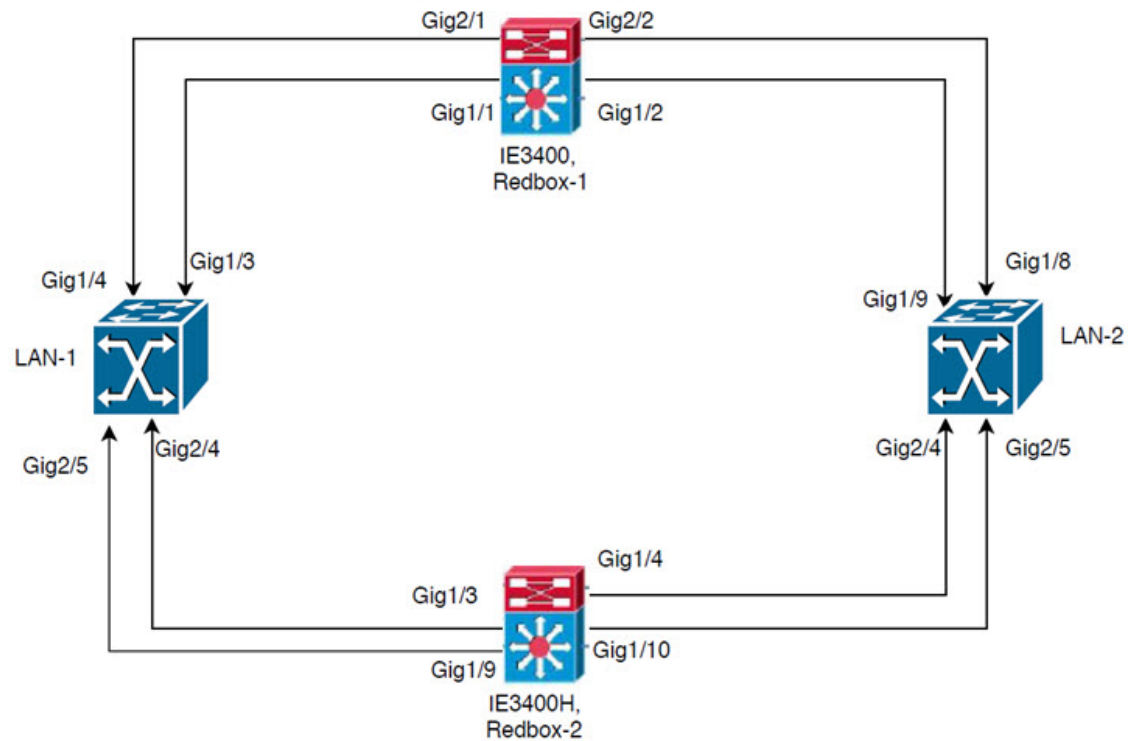
In this example, the configuration establishes two LANs, LAN-1 and LAN-2, and two PRP channels. Within the topology, an IE3400 is identified as Redbox-1 and an IE3400H is identified as Redbox-2.

Following is the configuration for LAN-1:

```
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
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

123

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

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

124

```
 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-2 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
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

125

```
 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
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

126

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
!
!
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 GigabitEthernet1/1
 switchport access vlan 35
 switchport mode access
 no ptp enable
 udld port disable
 no keepalive
 prp-channel-group 1
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/2
 switchport access vlan 35
 switchport mode access
 no ptp enable
 udld port disable
 no keepalive
 prp-channel-group 1
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

127

```
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4
 switchport access vlan 35
 switchport mode access
!
interface GigabitEthernet1/5
!
interface GigabitEthernet1/6
 description ***** tftp connection *****
 switchport access vlan 100
 switchport mode access
 shutdown
!
interface GigabitEthernet1/7
!
interface GigabitEthernet1/8
!
interface GigabitEthernet1/9
!
interface GigabitEthernet1/10
!
interface AppGigabitEthernet1/1
!
interface GigabitEthernet2/1
 switchport access vlan 25
 switchport mode access
 no ptp enable
 udld port disable
 no keepalive
 prp-channel-group 2
 spanning-tree bpdufilter enable
!
interface GigabitEthernet2/2
 switchport access vlan 25
 switchport mode access
 no ptp enable
 udld port disable
 no keepalive
 prp-channel-group 2
 spanning-tree bpdufilter enable
!
interface GigabitEthernet2/3
!
interface GigabitEthernet2/4
!
interface GigabitEthernet2/5
!
interface GigabitEthernet2/6
!
interface GigabitEthernet2/7
!
interface GigabitEthernet2/8
!
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
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

128

```
!
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
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

129

```
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/1
 shutdown
!
interface GigabitEthernet1/2
 shutdown
!
interface GigabitEthernet1/3
 switchport access vlan 35
 switchport mode access
 no ptp enable
 udld port disable
 no keepalive
 prp-channel-group 1
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/4
 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 GigabitEthernet1/9
 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 GigabitEthernet1/10
 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 GigabitEthernet1/11
!
interface GigabitEthernet1/12
!
interface GigabitEthernet1/13
!
interface GigabitEthernet1/14
!
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

130

```
interface GigabitEthernet1/15
!
interface GigabitEthernet1/16
!
interface GigabitEthernet1/17
!
interface GigabitEthernet1/18
!
interface GigabitEthernet1/19
!
interface GigabitEthernet1/20
!
interface GigabitEthernet1/21
!
interface GigabitEthernet1/22
!
interface GigabitEthernet1/23
!
interface GigabitEthernet1/24
!
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_IE3400#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
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

131

```
no platform bridge-security all
!
hostname PRP_IE3400
!
!
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
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

132

```
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 GigabitEthernet1/1
 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 GigabitEthernet1/2
 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 GigabitEthernet1/3
!
interface GigabitEthernet1/4
!
interface GigabitEthernet1/5
 shutdown
!
interface GigabitEthernet1/6
 switchport access vlan 197
 switchport mode access
!
interface GigabitEthernet1/7
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

133

```
!
interface GigabitEthernet1/8
!
interface GigabitEthernet1/9
!
interface GigabitEthernet1/10
 shutdown
!
interface AppGigabitEthernet1/1
!
interface GigabitEthernet2/1
 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 GigabitEthernet2/2
 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 GigabitEthernet2/3
!
interface GigabitEthernet2/4
!
interface GigabitEthernet2/5
!
interface GigabitEthernet2/6
!
interface GigabitEthernet2/7
!
interface GigabitEthernet2/8
!
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
!
!
!
!
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

134

```
!
!
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_IE3400#
```

Related Documents

- Cisco Catalyst IE3400 Rugged Series

- Cisco Catalyst IE3400 Heavy Duty Series

- IEC 62439-3, Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)

Feature History

Feature Name	Release	Feature Information
TrustSec Configuration on PRP Interface	Cisco IOS XE 17.13	Initial support on IE3x00.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

135

Feature Name	Release	Feature Information
PRP Supervision Frame VLAN Tagging	Cisco IOS XE 17.5	Initial support on IE3400 with IEM 3400 (Advanced Expansion) and IE3400H
PRP channel 2 support	Cisco IOS XE 17.4	Initial support on IE-3400 with IEM 3400 (Advanced Expansion) and IE3400H
Parallel Redundancy Protocol (1 PRP channel)	Cisco IOS XE 16.12.1	Initial support on IE-3400 with IEM 3400 (Advanced Expansion) and IE3400H

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

136

Configuring Resilient Ethernet Protocol

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfn.cloudapps.cisco.com/ITDIT/CFN/. An account on Cisco.com is not required.

Resilient Ethernet Protocol Overview

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

Note The feature is supported on Cisco Series Switches with the Network Essentials license.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

137

Note   REP configuration on downlink ports is supported starting with Cisco IOS XE Fuji 16.9.1.

REP segment is a chain of ports connected to each other and configured with a segment ID. Each segment consists of standard (non-edge) segment ports and two user-configured edge ports. A switch can have no more than two ports that belong to the same segment, and each segment port can have only one external neighbor. A segment can go through a shared medium, but on any link, only two ports can belong to the same segment. REP is supported only on Trunk ports.

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

Figure 15: REP Open Segment
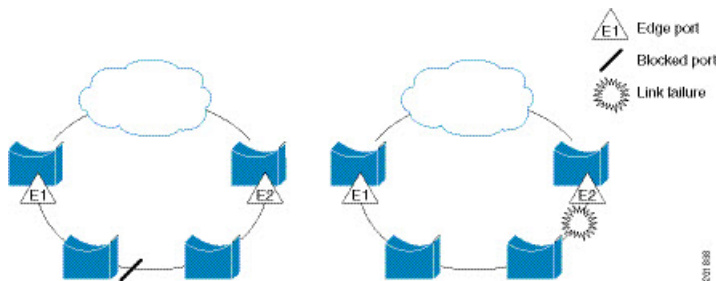
The segment shown in the figure above is an open segment; there is no connectivity between the two edge ports. The REP segment cannot cause a bridging loop, and you can safely connect the segment edges to any network. All hosts connected to switches inside the segment have two possible connections to the rest of the network through the edge ports, but only one connection is accessible at any time. If a failure occurs on any segment or on any port on a REP segment, REP unblocks the ALT port to ensure that connectivity is available through the other gateway.

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

Figure 16: REP Ring Segment
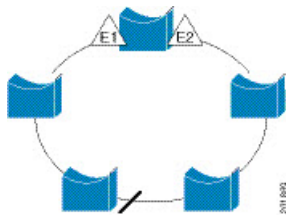
REP segments have the following characteristics:

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

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

138

- If a port is not operational, and cause a link failure, all ports forward traffic on all VLANs to ensure connectivity.

- In case of a link failure, alternate ports are unblocked as quickly as possible. When the failed link is restored, a logically blocked port per VLAN is selected with minimal disruption to the network.

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

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

Figure 17: Edge No-Neighbor Ports
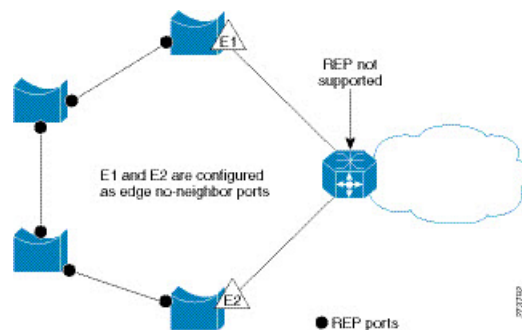
REP has these limitations:

- You must configure each segment port; an incorrect configuration can cause forwarding loops in the networks.

- REP can manage only a single failed port within the segment; multiple port failures within the REP segment cause loss of network connectivity.

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

Link Integrity

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

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

A segment port does not become operational if:

- No neighbor has the same segment ID.

- More than one neighbor has the same segment ID.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

139

• A neighbor does not acknowledge a local port as a peer.

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

Fast Convergence

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

VLAN Load Balancing

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

• By entering the port ID of the interface. To identify the port ID of a port in the segment, enter the **show interface rep detail** interface configuration command for the port.

• By entering the **preferred** keyword to select the port that you previously configured as the preferred alternate port with the **rep segment** *segment-id* **preferred** interface configuration command.

• By entering the neighbor offset number of a port in the segment, which identifies the downstream neighbor port of an edge port. The neighbor offset number range is –256 to +256; a value of 0 is invalid. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers indicate the secondary edge port (offset number -1) and its downstream neighbors.

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

The following figure shows neighbor offset numbers for a segment, where E1 is the primary edge port and E2 is the secondary edge port. The red numbers inside the ring are numbers offset from the primary edge port; the black numbers outside of the ring show the offset numbers from the secondary edge port. Note that you can identify all the ports (except the primary edge port) by either a positive offset number (downstream position from the primary edge port) or a negative offset number (downstream position

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

140

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

Figure 18: Neighbor Offset Numbers in a Segment
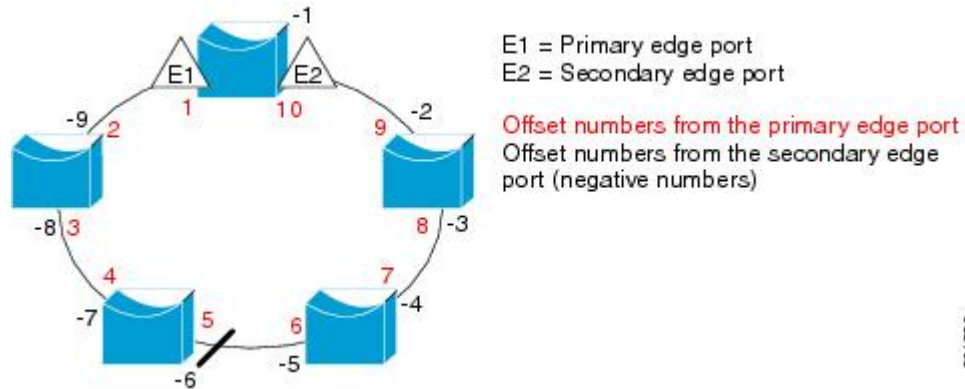
When the REP segment is complete, all the VLANs are blocked. When you configure VLAN load balancing, you must also configure triggers in one of two ways:

- Manually trigger VLAN load balancing at any time by entering the **rep preempt segment** *segment-id* privileged EXEC command on the switch that has the primary edge port.

- Configure a preempt delay time by entering the **rep preempt delay** *seconds* interface configuration command. After a link failure and recovery, VLAN load balancing begins after the configured preemption time period elapses. Note that the delay timer restarts if another port fails before the time has elapsed.

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

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

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

Reconfigure the primary edge port to reconfigure load balancing. When you change the load-balancing configuration, the primary edge port waits for the **rep preempt segment** command or for the configured preempt delay period after a port failure and recovery, before executing the new configuration. If you change an edge port to a regular segment port, the existing VLAN load-balancing status does not change. Configuring a new edge port might cause a new topology configuration.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

141

Spanning Tree Interaction

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

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

Resilient Ethernet Protocol (REP) Negotiated

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

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

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

- The new switch will cause a break in the REP ring.

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

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

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

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

- **STP**: By default, STP is enabled on all the ports on the Cisco Switch.

- **REP**: The customer network is configured to form a REP ring to provide better convergence time and redundancy.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

142

- **Cisco Discovery Protocol (CDP)**: The feature depends on user defined TLVs sent through CDP messages to negotiate the correct (STP or REP) configuration for the interface.

REP Ports

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

- A port configured as a regular segment port starts as a failed port.

- After the neighbor adjacencies are determined, the port transitions to alternate port state, blocking all the VLANs on the interface. Blocked-port negotiations occur, and when the segment settles, one blocked port remains in the alternate role and all the other ports become open ports.

- When a failure occurs in a link, all the ports move to the Failed state. When the Alternate port receives the failure notification, it changes to the Open state, forwarding all the VLANs.

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

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

REP Fast Overview

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

REP was originally designed for Fast Ethernet (FE 10/100) ports. Link down detection time on FE ports is 10 milliseconds (ms) and convergence time is about 50 ms. On Fiber GE ports, link down time is 10 ms, but on GE copper interfaces, the link drop detection and recovery times are between 750 ms and 350 ms. As a result, link loss and recovery can be detected a lot more quickly on GE fiber interfaces than on corresponding copper interfaces. This in turn means that the convergence time for REP is a lot higher when using GE copper interfaces.

To improve link down detection time, a beacon mechanism is implemented to trigger faster link failure detection (within 5-10 ms) when a REP interface is configured for REP Fast mode. The switch has two timers for each REP interface. The first timer is triggered every 3 ms to transmit the beacon frame to the neighbor node. After successful transmission and reception of the frame, both the timers are reset. If the packet is not received after the transmission, then the second timer is triggered to check the reception within 10 ms. If the packet is not received, upon the timer expiry, a link down message is sent to the switch.

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

A REP Ring can have a mix of normal REP links and links with REP Fast. Interfaces with REP Fast will transmit 3000 packets a second as part normal operation. REP Fast enablement does not impact REP ring size

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

143

since it operates only on the pair of interfaces configured for it. Because REP Fast has to generate Beacon frames, only six interfaces on a single REP node can be configured for REP Fast at a time.

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

To configure REP Fast, see .

REP Zero Touch Provisioning

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

REP and Day Zero

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

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

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

144

Figure 19: Adding Edge Nodes to the REP Ring
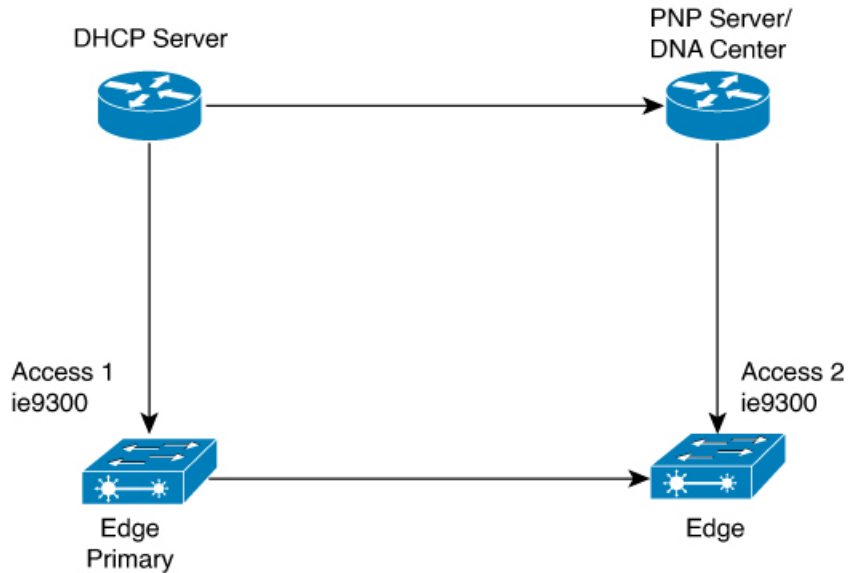
Note The DHCP Server and the PnP Server/DNA Center are not part of the REP ring.

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

Figure 20: Adding Downstream Nodes

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches ■

145
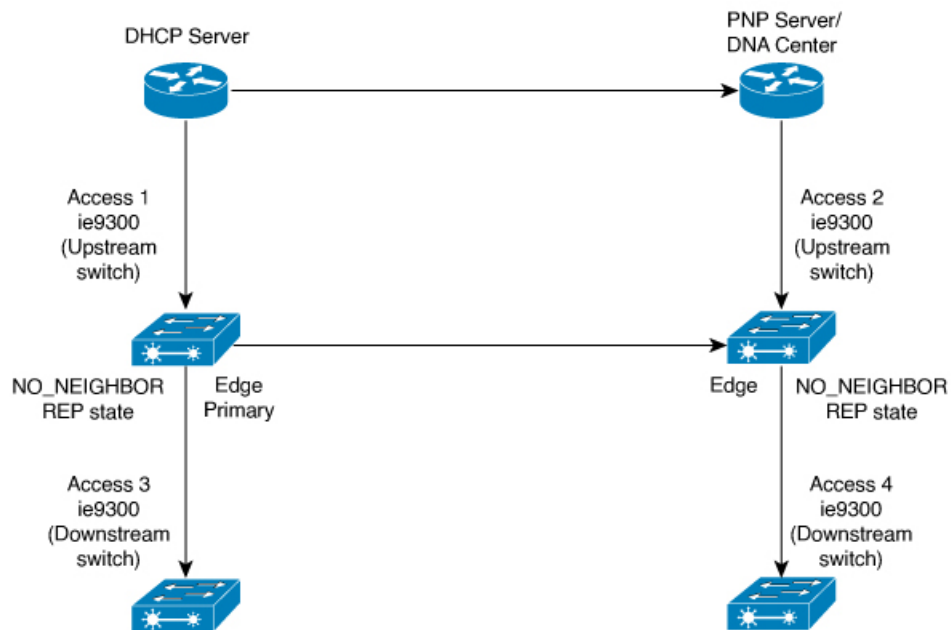
When either Access 3 or Access 4 are powered on, the REP edge primary port starts the REP protocol negotiation and discovers that the neighbor port is not a REP enabled port. (Recall that the switch will be added to the REP ring only after PnP provisioning, for which it needs to first contact the DHCP server as explained earlier.) When an upstream switch port has REP configured and a downstream switch is getting on-boarded with PnP, the REP port goes into the NO_NEIGHBOR state because it is not able to discover its REP peer. In the NO_NEIGHBOR state, REP blocks all the VLANs on that port. This means that the DHCP discovery message from the new switch on the PnP startup VLAN is dropped by the upstream switch because its REP state is NO_NEIGHBOR. The same sequence of blocked ports continues for all new switches added to the REP ring (see Access 5 in figure below).

Figure 21: NO_NEIGHBOR REP State
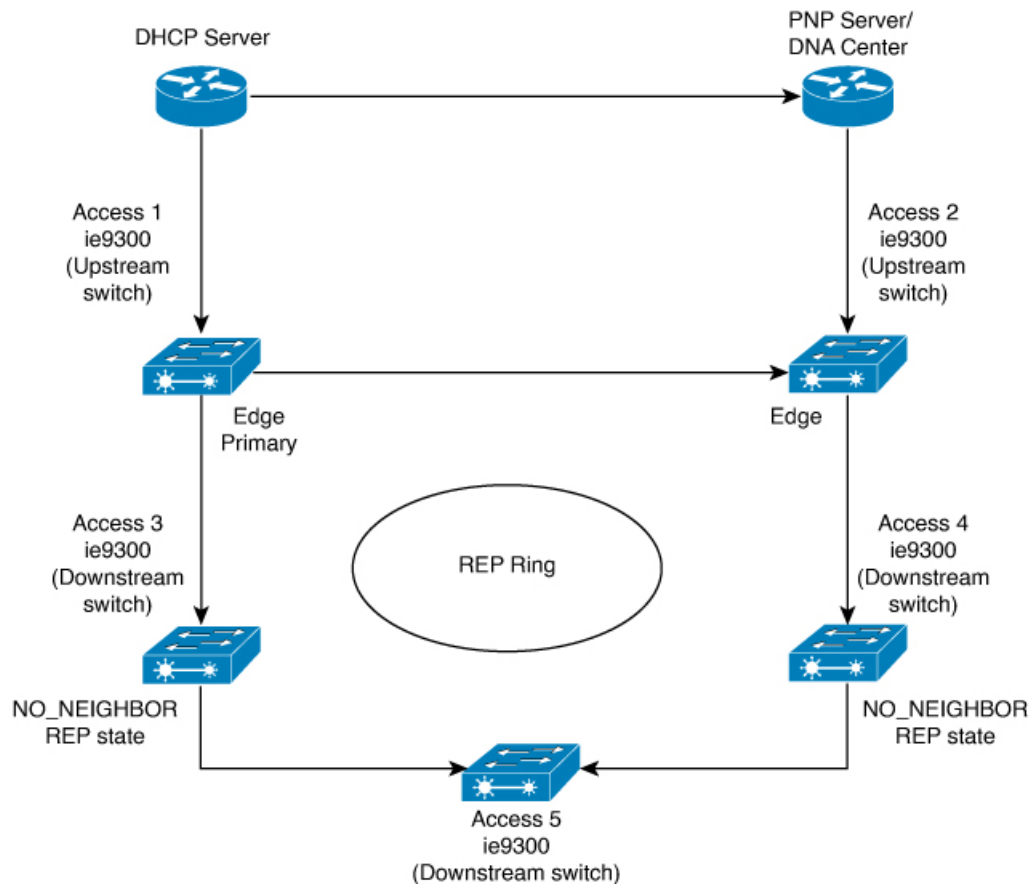
REP ZTP Overview

The REP ZTP enhancements require that both the upstream and the downstream switches support the feature. When the new downstream switch is powered on, it initiates PNP/autoinstall. The upstream switch's interface is configured for REP and blocks the interface to the downstream switch because the downstream switch is not REP by default (the upstream switch is in REP_NO_NEIGHBOR state).

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

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

146

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

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

The downstream behavior to transmit the REP LSL with new TLV to request the PnP startup VLAN be unblocked is the default behavior for switches with no startup configuration. For security purposes, the upstream switch must have the interface to the downstream switch explicitly enabled to put the PnP startup VLAN into unblocked state. The interface level command is **rep ztp-enable**. See Configuring REP ZTP, on page 158.

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

REP Segment-ID Autodiscovery

Resilient Ethernet Protocol (REP) Segment-ID Autodiscovery enables automatic configuration and continued static configuration of segment IDs in REP segments. The feature is supported on Cisco Catalyst IE3x00 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches beginning with the Cisco IOS XE Cupertino 17.9.x release.

A REP segment is a chain of ports that are connected to each other and configured with a segment ID. Forming multiple REP segments statically by configuring each port of the device is a manual task, and any mismatch in configuring the segment ID leads to convergence issues. However, REP Segment-ID Autodiscovery adds new CLI commands to enable a switch to learn and retain segment ID information automatically.

You can use REP Segment-ID Autodiscovery in several different scenarios. You can insert a new switch into an existing REP segment or in a new REP segment that you build yourself. The feature is ideal for multiple REP ring deployments when incorrect REP Segment IDs might be entered manually. Such errors can occur when deploying multiple REP rings from the same REP seed node.

See the following sections in this guide for more information:

- REP Segment-ID Autodiscovery Deployment
- Configuring REP Segment-ID Autodiscovery

REP Segment-ID Autodiscovery Deployment

You can configure REP Segment-ID Autodiscovery when you add a switch to a REP segment or when you create a REP segment. In either case, the feature reduces the amount of manual configuration that you must do.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches ■

147

Adding a new Switch to an REP Segment

When you add a switch to an existing REP segment, you enable autodiscovery by entering the **rep autodisc** command on the switch interfaces connecting to the upstream and downstream switches.

When the new switch is connected to the upstream and downstream switches, the upstream and downstream switches send CDP packets with REP segment ID information to the new switch interfaces. You enter the command **rep segment auto** on the new switch interfaces so they can learn the segment ID.

Building a new REP Segment

When you build a closed REP segment, you must start with a static REP segment ID configuration from an edge device. The primary and secondary edge devices in a closed segment are on the same switch. When you build an open REP segment, you must start a static REP segment ID configuration from both primary and secondary edge devices.

The remaining steps are the same for both closed and open REP segments. You bring up the next node in the REP ring. You then add any next new node between these two switches for autodiscovery to work correctly.

Building a REP Segment with Uplinks

When you build a ring segment with uplinks (daisy chain), you must start with a static REP segment ID configuration from the REP edge node. Connect the next device to one of the uplinks to the edge node, and enable autodiscovery on the connected uplink. Because of port pairing support, the same REP configuration is duplicated on the paired uplink port.

When the next device is connected with the uplink, the process repeats to bring the REP segment in a daisy chain manner. Each new REP node automatically joins the ring by learning the REP Segment ID from the node above it. For a REP open ring, the last device on the segment is an edge device with static REP configuration.

REP Segment-ID Autodiscovery Limitations

The following are restrictions for the REP Segment-ID Autodiscovery feature:

- The only supported port-pairing is uplinks Gi1/1 and Gi1/2. No predefined port pairing is supported for downlinks.

  If you configure a REP segment on a downlink port, the switch receives the segment ID from the upstream switch, and the partner downlink port is connected to the same segment. However, the switch does not pass the segment ID to its partner port. Instead, you must explicitly configure the partner port of the downlink pair.

- The REP Segment-ID Autodiscovery feature is not supported when you insert an edge node into the existing segment. You must configure static or manual REP segment ID on primary and secondary edge devices.

- If you insert a new switch between two switches that are part of a segment, you must connect the new switch interfaces to the interfaces of existing switches that transmit the same segment ID. Any incorrect connections to other interfaces of the existing switches leads to segment failure.

  For example, assume gi1/1 of switch1 and gi1/2 of switch2 are connected as a part an existing segment, and switch3 is inserted between these two switches. In such a case, you must ensure that the interfaces are connected to gi1/1 of switch1 and gi1/2 of switch2 to include switch3 as a part of the same segment.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

148

- If you configure REP automatically on an interface with the **rep segment auto** command, and you remove the REP configuration with the **no rep segment** command or overwrite it with the **rep segment <>** command, you cannot configure REP automatically again with the **rep segment auto** command. Instead, you must shut down the interface, bring it up, and then enter the **rep segment auto** command.

- REP Segment ID Autodiscovery depends on the CDP protocol. The feature does not support EtherChannel links.

How to Configure Resilient Ethernet Protocol

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

Default REP Configuration

- REP is disabled on all the interfaces. When enabled, the interface is a regular segment port unless it is configured as an edge port.

- When REP is enabled, the task of sending segment topology change notices (STCNs) is disabled, all the VLANs are blocked, and the administrative VLAN is VLAN 1.

- When VLAN load balancing is enabled, the default is manual preemption with the delay timer disabled. If VLAN load balancing is not configured, the default after manual preemption is to block all the VLANs in the primary edge port.

- REP Fast is disabled by default.

- REP Zero Touch Provisioning is enabled by default at the global level and disabled at the interface level.

REP Configuration Guidelines

Follow these guidelines when configuring REP:

- We recommend that you begin by configuring one port and then configure contiguous ports to minimize the number of segments and the number of blocked ports.

- If more than two ports in a segment fail when no external neighbors are configured, one port goes into a forwarding state for the data path to help maintain connectivity during configuration. In the **show interfaces rep** command output, the Port Role for this port shows as "Fail Logical Open;" and the Port Role for the other failed port shows as "Fail No Ext Neighbor." When the external neighbors for the failed ports are configured, the ports go through the alternate port state transitions and eventually go to an open state or remain as the alternate port, based on the alternate port selection mechanism.

- REP ports must be Layer 2 IEEE 802.1Q or Trunk ports.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

149

- We recommend that you configure all trunk ports in the segment with the same set of allowed VLANs.

- Be careful when configuring REP through a Telnet connection. Because REP blocks all VLANs until another REP interface sends a message to unblock it. You might lose connectivity to the router if you enable REP in a Telnet session that accesses the router through the same interface.

- You cannot run REP and STP on the same segment or interface.

- If you connect an STP network to a REP segment, be sure that the connection is at the segment edge. An STP connection that is not at the edge could cause a bridging loop because STP does not run on REP segments. All STP BPDUs are dropped at REP interfaces.

- If REP is enabled on two ports on a switch, both ports must be either regular segment ports or edge ports. REP ports follow these rules:

  - There is no limit to the number of REP ports on a switch; however, only two ports on a switch can belong to the same REP segment.

  - If only one port on a switch is configured in a segment, the port should be an edge port.

  - If two ports on a switch belong to the same segment, they must be both edge ports, both regular segment ports, or one regular port and one edge no-neighbor port. An edge port and regular segment port on a switch cannot belong to the same segment.

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

- REP interfaces come up in a blocked state and remain in a blocked state until they are safe to be unblocked. You must be aware of this status to avoid sudden connection losses.

- REP sends all LSL PDUs in untagged frames on the native VLAN. The BPA message sent to the Cisco multicast address is sent on the administration VLAN, which is VLAN 1 by default.

- You can configure how long a REP interface remains up without receiving a hello from a neighbor. You can use the **rep lsl-age-timer** value interface configuration command to set the time from 120 ms to 10000 ms. The LSL hello timer is then set to the age-timer value divided by 3. In normal operation, three LSL hellos are sent before the age timer on the peer switch expires and checks for hello messages.

  - EtherChannel port channel interfaces do not support LSL age-timer values less than 1000 ms. If you try to configure a value less than 1000 ms on a port channel, you receive an error message and the command is rejected.

  - **lsl-age-timer** is intended to be used when normal link down detection will be too slow for convergence time.

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

- You cannot configure REP ports as one of the following port types:

  - Switched Port Analyzer (SPAN) destination port

  - Tunnel port

  - Access port

- REP is supported on EtherChannels, but not on an individual port that belongs to an EtherChannel.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

150

- There can be a maximum of 26 REP segments per switch.

- There is no limit to the size of a REP ring. REP ring sizes greater than 20 nodes may not achieve sub 50ms convergence. The use of REP ZTP or REP Segment ID Autodiscovery limits a single node to only three REP segments.

REP Fast

- REP fastmode cannot co-exist with MACsec. This restriction applies to the IE3x00 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches.

  REP fastmode sends a beacon before a link comes up, for faster convergence, and it keeps the port down until the beacon is detected. MKA negotiation cannot take place before the link is up, and by design MACsec configuration drops everything except for EAPOL packets until the MKA session is secured. This means that with the combination of REP fastmode and MACsec, REP fast beacons are dropped and MKA negotiation does not occur.

  MACsec with REP works as expected.

REP Zero Touch Provisioning

- REP ZTP requires the PnP feature to be present on Cisco Catalyst IE 200, IE3300, and IE3400 series switches.

- REP behavior during the NO_NEIGHBOR state is modified beginning in in Cisco IOS XE 17.8.1 and later. This transient state change in port forwarding behavior in NO_NEIGHBOR state allows a DHCP request message to reach a DHCP server and unblock PnP provisioning of a new switch. There should not be any impact to the REP state machine after PnP completion.

- The changes in REP behavior during the NO_NEIGHBOR state apply only to REP Zero Touch Provisioning (ZTP) in Cisco IOS XE 17.8.1 and later. If the PnP feature is not present, normal REP functionality should work as expected.

- The REP ZTP feature coexists with REP bpduleak/negotiated feature on fiber uplink ports.

- The REP ZTP feature is not supported on EtherChannel interfaces for day 0 on an upstream switch because EtherChannel is not present on the downstream interface by default. REP ZTP works only on physical interfaces.

- REP ZTP is supported on both copper (downlink) and fiber (uplink) interfaces.

- REP ZTP is interoperable only with other IE switching products running IOS XE that claim REP ZTP support.

Configuring REP Administrative VLAN

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

Follow these guidelines when configuring the REP administrative VLAN:

- If you do not configure an administrative VLAN, the default is VLAN 1.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

151

• You can configure one admin VLAN on the switch for all segments.

• The administrative VLAN cannot be the RSPAN VLAN.

To configure the REP administrative VLAN, follow these steps, beginning in privileged EXEC mode:

Procedure

	Command or Action	**Purpose**
Step 1	**enable** **Example:** Device> **enable**	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# **configure terminal**	Enters global configuration mode.
Step 3	**rep admin vlan** *vlan-id* **Example:** Device(config)# **rep admin vlan 2**	Specifies the administrative VLAN. The range is from 2 to 4094. To set the admin VLAN to 1, which is the default, enter the **no rep admin vlan** global configuration command.
Step 4	**end** **Example:** Device(config)# **end**	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	**show interface** [*interface-id*] **rep detail** **Example:** Device# **show interface gigabitethernet1/1 rep detail**	(Optional) Verifies the configuration on a REP interface.
Step 6	**copy running-config startup config** **Example:** Device# **copy running-config startup config**	(Optional) Saves your entries in the switch startup configuration file.

Configuring a REP Interface

To configure REP, enable REP on each segment interface and identify the segment ID. This task is mandatory, and must be done before other REP configurations. You must also configure a primary and secondary edge port on each segment. All the other steps are optional.

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

Procedure

	Command or Action	**Purpose**
Step 1	**enable**	Enables privileged EXEC mode.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

152

	Command or Action	Purpose
	Example: Device> **enable**	Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# **configure terminal**	Enters global configuration mode.
Step 3	**interface** *interface-id* **Example:** Device(config)# **interface gigabitethernet1/1**	Specifies the interface, and enters interface configuration mode. The interface can be a physical Layer 2 interface or a port channel (logical interface).
Step 4	**switchport mode trunk** **Example:** Device(config-if)# **switchport mode trunk**	Configures the interface as a Layer 2 trunk port.
Step 5	**rep segment** *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**] **Example:** Device(config-if)# **rep segment 1 edge no-neighbor primary**	Enables REP on the interface and identifies a segment number. The segment ID range is from 1 to 1024. **Note** You must configure two edge ports, including one primary edge port, for each segment. These optional keywords are available: • (Optional) **edge**—Configures the port as an edge port. Each segment has only two edge ports. Entering the keyword **edge** without the keyword **primary** configures the port as the secondary edge port. • (Optional) **primary**—Configures the port as the primary edge port, the port on which you can configure VLAN load balancing. • (Optional) **no-neighbor**—Configures a port with no external REP neighbors as an edge port. The port inherits all the properties of an edge port, and you can configure the properties the same way you would for an edge port. **Note** Although each segment can have only one primary edge port, if you configure edge ports on two different switches and enter the keyword **primary** on both the switches, the configuration is valid. However, REP selects only one of these ports as the segment primary edge port. You can identify the primary edge port for a segment by entering the **show rep topology** command in privileged EXEC mode.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

153

	Command or Action	**Purpose**
		• (Optional) **preferred**—Indicates that the port is the preferred alternate port or the preferred port for VLAN load balancing.
		Note Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives the port a slight edge over equal contenders. The alternate port is usually a previously failed port.
Step 6	**rep stcn** {**interface** *interface id* | **segment** *id-list* | **stp**} **Example:** Device(config-if)# **rep stcn segment 25-50**	(Optional) Configures the edge port to send segment topology change notices (STCNs). • **interface** *interface-id*—Designates a physical interface or port channel to receive STCNs. • **segment** *id-list*—Identifies one or more segments to receive STCNs. The range is from 1 to 1024. • **stp**—Sends STCNs to STP networks. **Note** Spanning Tree (MST) mode is required on edge no-neighbor nodes when **rep stcn stp** command is configured for sending STCNs to STP networks.
Step 7	**rep block port** {**id** *port-id* | *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**} **Example:** Device(config-if)# **rep block port id 0009001818D68700 vlan 1-100**	(Optional) Configures VLAN load balancing on the primary edge port, identifies the REP alternate port in one of three ways (**id** *port-id*, *neighbor_offset*, **preferred**), and configures the VLANs to be blocked on the alternate port. • **id** *port-id*—Identifies the alternate port by port ID. The port ID is automatically generated for each port in the segment. You can view interface port IDs by entering the **show interface** *type number* **rep** [**detail**] privileged EXEC command. • *neighbor_offset*—Number to identify the alternate port as a downstream neighbor from an edge port. The range is from -256 to 256, with negative numbers indicating the downstream neighbor from the secondary edge port. A value of **0** is invalid. Enter **-1** to identify the secondary edge port as the alternate port. **Note** Because you enter the **rep block port** command at the primary edge port (offset number 1), you cannot enter an offset value of 1 to identify an alternate port. • **preferred**—Selects the regular segment port previously identified as the preferred alternate port for VLAN load balancing.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

154

Command or Action	Purpose
	• **vlan** *vlan-list*—Blocks one VLAN or a range of VLANs.
	• **vlan all**—Blocks all the VLANs.
	Note Enter this command only on the REP primary edge port.
Step 8 **rep preempt delay** *seconds* **Example:** Device(config-if)# **rep preempt delay 100**	(Optional) Configures a preempt time delay. • Use this command if you want VLAN load balancing to be automatically triggered after a link failure and recovery. • The time delay range is between15 to 300 seconds. The default is manual preemption with no time delay. **Note** Enter this command only on the REP primary edge port.
Step 9 **rep lsl-age-timer** *value* **Example:** Device(config-if)# **rep lsl-age-timer 2000**	(Optional) Configures a time (in milliseconds) for which the REP interface remains up without receiving a hello from a neighbor. The range is from 120 to 10000 ms in 40-ms increments. The default is 5000 ms (5 seconds). **Note** • EtherChannel port channel interfaces do not support LSL age-timer values that are less than 1000 ms. • Both the ports on the link should have the same LSL age configured in order to avoid link flaps.
Step 10 **end** **Example:** Device(config-if)# **end**	Exits global configuration mode and returns to privileged EXEC mode.
Step 11 **show interface** [*interface-id*] **rep** [**detail**] **Example:** Device# **show interface gigabitethernet1/1 rep detail**	(Optional) Displays the REP interface configuration.
Step 12 **copy running-config startup-config** **Example:** Device# **copy running-config startup-config**	(Optional) Saves your entries in the router startup configuration file.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

155

Setting Manual Preemption for VLAN Load Balancing

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

Procedure

	Command or Action	**Purpose**
Step 1	**enable**	Enables privileged EXEC mode.
	Example:	Enter your password if prompted.
	Device> **enable**	
Step 2	**rep preempt segment** *segment-id*	Manually triggers VLAN load balancing on the segment.
	Example:	You need to confirm the command before it is executed.
	Device# **rep preempt segment 100** The command will cause a momentary traffic disruption. Do you still want to continue? [confirm]	
Step 3	**show rep topology segment** *segment-id*	(Optional) Displays REP topology information.
	Example:	
	Device# **show rep topology segment 100**	
Step 4	**end**	Exits privileged EXEC mode.
	Example:	
	Device# **end**	

Configuring SNMP Traps for REP

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

Procedure

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

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

156

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

Configuring REP Fast

Follow these steps to configure REP Fast:

Before you begin

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

Step 1 Enter global configuration mode:

configure terminal

Step 2 Specify the interface and enter interface configuration mode:

interface *interface-id*

Step 3 Enable REP Fast:

rep fastmode

Step 4 Return to priviledged exec mode:

end

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

157

Example

```
Switch# configure terminal
Switch(config)# int gi 1/4
Switch(config-if#) rep segment 1 edge
Switch(config-if)# rep fastmode
Switch(config-if)# end
Switch# sh run int gi 1/4
interface GigabitEthernet1/4
switchport trunk allowed vlan 1-10
switchport mode trunk
rep segment 1 edge
rep fastmode
```

Configuring REP ZTP

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

- Global level: Enabled

- Interface level: Disabled

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

Note When applying configuration from DNAC or PNP server user must explicitly add this CLI configuration in the configuration template for the feature to be enabled.

Step 1 Enter global configuration mode:

Switch# **configure terminal**

Step 2 Globally enable REP ZTP:

Switch(config)# **rep ztp**

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

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

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

Step 4 Enable REP ZTP on the interface:

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

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

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

158

Example

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

```
Switch#show running-config interface gigabitEthernet 1/2
Building configuration...

Current configuration : 93 bytes
!
interface GigabitEthernet1/2
 switchport mode trunk
 rep segment 100
 rep ztp-enable
end
```

Configuring REP Segment-ID Autodiscovery

You use CLI commands tor REP Segment-ID Autodiscovery. One enables or disables autodiscovery on a REP switch, and one configures new interfaces so the switch learns the segment-ID. You also use CLI commands to view the status of the feature on the segment.

Enable REP Segment-ID Autodiscovery

REP Segment-ID Autodiscovery is enabled by default. However, you can re-enable it on the switch upstream and downstream interfaces.

Enable REP Segment-ID Autodiscovery on the switch.

Example:

```
switch(config)#rep autodisc
```

You disable REP Segment-ID Autodiscovery by entering the following command:

```
switch(config)#no rep autodisc
```

What to do next

You can check the status of REP Segment-ID Autodiscovery. See the section in this guide.

Configure the Interfaces

Configure the interface on the newly inserted switch so that downstream nodes to participate in the REP segment. The **rep segment auto** command automatically fetches the segment ID from the upstream switch.

Before you begin

Ensure that the REP segment ID is configured on the primary and secondary edge devices. You configure the segment ID by entering the command **rep segment** *segment_id* **edge**, in which *segment_id* is the segment ID of the ring to be propagated through CDP packet to the neighboring device when connected.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

159

Enable the switch to learn the segment ID.

Example:

```
switch(config)#int gig1/1
switch(config-if)#rep seg auto
```

Note Cisco IOS XE Cupertino 17.9.1 and later releases support port pairing for uplinks. That is, when you configure **rep segment auto** on one of the uplinks, the same configuration is made automatically on the other uplink.

However, port pairing is *not* supported for downlinks. You must configure each downlink separately.

Following example shows the minimum configuration to enable the feature on an interface on the upstream device switch. The upstream device with an explicit REP segment is typically an edge switch.

```
switch#show running-config interface gigabitEthernet 1/3
Building configuration...

Current configuration : 93 bytes
!
interface GigabitEthernet1/3
 switchport mode trunk
 rep segment auto 1
```

The following example shows the minimum configuration to enable the feature on an interface on the downstream switch interface. Enter the command **show running-config interface** *interface_id* to confirm that the downstream switch knows to expect to receive its REP segment through CDP message.

```
switch#show running-config interface gigabitEthernet 1/2
Building configuration...

Current configuration : 93 bytes
!
interface GigabitEthernet1/2
 switchport mode trunk
 rep segment auto
end
```

You disable the ability of the switch to learn the segment ID by entering the following command:

```
switch(config-if)#no rep segment
```

What to do next

You can check the status of REP Segment-ID Autodiscovery. See the section View Feature Status, on page 160 in this guide.

View Feature Status

You can use CLI commands to check the status of REP Segment-ID Autodiscovery on the segment.

Confirm that REP Segment-ID Autodiscovery is globally enabled on the switch.

Example:

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

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

160

The following examples show other commands for checking the status of REP Segment-ID Autodiscovery:

• The following example shows the command to check if the feature is globally disabled on a device:

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

• The following example shows the command to confirm that the segment ID on interface is configured automatically:

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

• The following example shows the command to confirm that the segment ID on the interface is configured manually:

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

Monitoring Resilient Ethernet Protocol Configurations

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

```
Device# show interfaces GigabitEthernet1/4 rep detail

GigabitEthernet1/4 REP enabled
Segment-id: 3 (Primary Edge)
PortID: 03010015FA66FF80
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 02040015FA66FF804050
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
REP-ZTP Status: Disabled
Preempt Delay Timer: disabled
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 999, tx: 652
HFL PDU rx: 0, tx: 0
BPA TLV rx: 500, tx: 4
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 6, tx: 5
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 135, tx: 136
```

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

```
Device#show interface GigabitEthernet1/5 rep detail
GigabitEthernet1/5   REP enabled
Segment-id: 1 (Segment)
PortID: 019B380E4D9ACAC0
Preferred flag: No
Operational Link Status: NO_NEIGHBOR
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

161

```
Current Key: 019B380E4D9ACAC0696B
Port Role: Fail No Ext Neighbor
Blocked VLAN: 1-4094
Admin-vlan: 1
REP-ZTP Status: Disabled
Preempt Delay Timer: 100 sec
LSL Ageout Timer: 2000 ms
LSL Ageout Retries: 5
Configured Load-balancing Block Port: 09E9380E4D9ACAC0
Configured Load-balancing Block VLAN: 1-100
STCN Propagate to: segment 25
LSL PDU rx: 292, tx: 340
HFL PDU rx: 0, tx: 0
BPA TLV rx: 0, tx: 0
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 0, tx: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 0, tx: 0
```

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

```
Device# show rep topology

REP Segment 1
BridgeName       PortName    Edge Role
---------------- ----------  ---- ----
10.64.106.63     Gi1/4       Pri  Open
10.64.106.228    Gi1/4            Open
10.64.106.228    Gi1/3            Open
10.64.106.67     Gi1/3            Open
10.64.106.67     Gi1/4            Alt
10.64.106.63     Gi1/4       Sec  Open

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

Displaying REP Fast Beacon Information

When REP Fast is enabled, the system sends beacon frames to the neighbor node for link status detection. Use the following command to display the number of beacon frames sent and received on an interface.

In priviledged exec mode, enter:

show platform rep beacon interface *interface-id*

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

162

Example

```
Switch# sh platform rep beacon GigabitEthernet 1/4
Beacon RX : 43984
Beacon TX : 46826
```

Investigating Broken Links

This section explains how to interpret **show rep topology** output if a link failure occurs.

Here is an example of a REP closed ring:

Figure 22: REP Closed Ring Topology
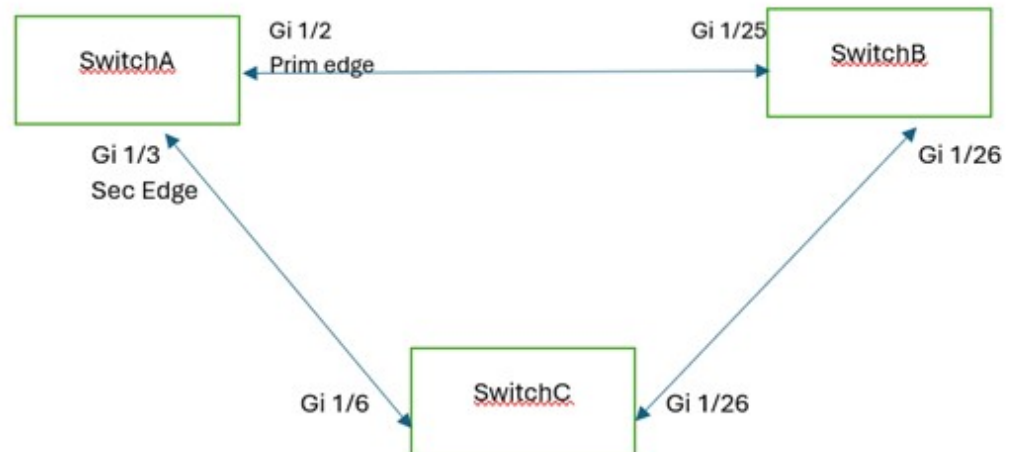

```
SWITCHA#sh rep topology
REP Segment 1
BridgeName                        PortName   Edge Role
--------------------------------- ---------- ---- ----
SWITCHA                           Gi1/2      Pri  Open
SWITCHB                           Gi1/25          Open
SWITCHB                           Gi1/26          Open
SWITCHC                           Gi1/26          Open
SWITCHC                           Gi1/6           Open
SWITCHA                           Gi1/3      Sec  Alt
```

Here is an example where the connection between SwitchB and SwitchC is down:

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

163

Figure 23: REP Closed Ring Topology with Link Failure
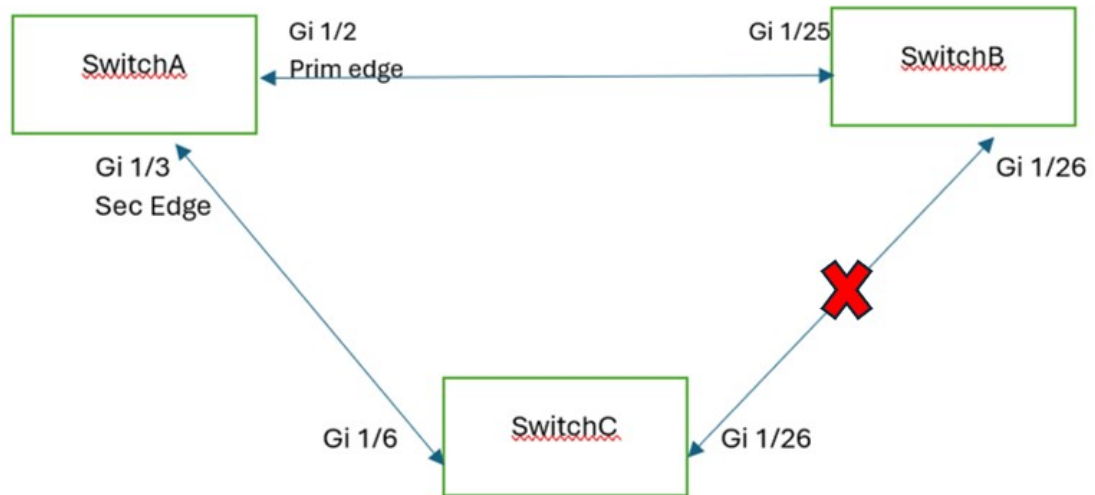

```
SWITCHA#sh rep topology
REP Segment 1
Warning: REP detects a segment failure, topology may be incomplete

BridgeName                        PortName    Edge Role
-------------------------------- ---------- ---- ----
SWITCHA                           Gi1/2       Sec  Open
SWITCHB                           Gi1/25           Open
SWITCHB                           Gi1/26           Fail
```

The **show rep topology** output relies on a database built using Edge Port Advertisement (EPA) packets. Each node in the ring is expected to receive two EPA packets, one each from the Primary and Secondary edge ports. Each port adds its own topology information to the topology information that it received.

If a failure in the topology occurs, depending on where the link failure is in relation to a node's position, the node will have a limited view of the topology starting from the connected edge port up to the node (as shown in the example **show rep topology** output above where a failure has occurred). In this case the node fails to transmit the EPA packets, resulting in each node showing different topology information in the **show rep topology** output.

Note   This behavior is limited to the **show rep topology** command output only. The data path is not affected.

Displaying REP ZTP Status

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

Step 1   In priviledged exec mode, enter:

show interfaces rep detail

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

164

Example:

```
GigabitEthernet1/1   REP enabled
Segment-id: 100 (Segment)
PortID: 00016C13D5AC4320
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 00026C13D5AC43209DAB
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
REP-ZTP Status: Disabled
REP Segment Id Auto Discovery Status: Enabled
REP Segment Id Type: Manual
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
LSL Ageout Retries: 5
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 382, tx: 297
HFL PDU rx: 0, tx: 0
BPA TLV rx: 1, tx: 19
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 95, tx: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 95, tx: 95

GigabitEthernet1/2   REP enabled
Segment-id: 100 (Segment)
PortID: 00026C13D5AC4320
Preferred flag: No
Operational Link Status: NO_NEIGHBOR
Current Key: 00026C13D5AC43209DAB
Port Role: Fail No Ext Neighbor
Blocked VLAN: 1-4094
Admin-vlan: 1
REP-ZTP Status: Enabled
REP-ZTP PnP Status: Unknown
REP-ZTP PnP Vlan: 1
REP-ZTP Port Status: Blocked
REP Segment Id Auto Discovery Status: Enabled
REP Segment Id Type: Manual
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
LSL Ageout Retries: 5
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 11, tx: 11
HFL PDU rx: 0, tx: 0
BPA TLV rx: 0, tx: 0
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 0, tx: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 0, tx: 0
```

Step 2   Use the show command again to display the status of **pnp_startup_vlan**.

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

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

165

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

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

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

Example:

```
Switch#show interfaces rep detail
GigabitEthernet1/1    REP enabled
Segment-id: 100 (Segment)
PortID: 00016C13D5AC4320
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 00026C13D5AC43209DAB
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
REP-ZTP Status: Disabled
REP Segment Id Auto Discovery Status: Enabled
REP Segment Id Type: Manual
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
LSL Ageout Retries: 5
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 430, tx: 358
HFL PDU rx: 0, tx: 0
BPA TLV rx: 1, tx: 67
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 107, tx: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 107, tx: 108

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

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

166

```
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 0, tx: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 0, tx: 0
```

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

Example:

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

Step 4 (Optional) Use the following debug commands to troubleshoot REP ZTP:

• **debug rep lslsm**: This command helps you understand LSL state machine events in the NO_NEIGHBOR state.

• **debug rep packet**: Use this command to dump LSL packets with the REP ZTP LSL TLV to check the PnP status on the peer client node.

Additional References for Resilient Ethernet Protocol

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use the Cisco MIB Locator found at: https://mibs.cloudapps.cisco.com/ITDIT/MIBS/MainServlet

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

167

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	https://www.cisco.com/c/en/us/support/index.html?ts=AZ6NHYKB9WRPLYAVGST1587714574492

Feature History

Feature Name	Release	Feature Information
REP Zero Touch Provisioning	Cisco IOS XE 17.8.1	Initial support on Cisco Catalyst IE 3200, 3300, and 3400
REP Negotiated	Cisco IOS XE 16.12.1	Initial support on Cisco Catalyst IE 3200, 3300, and 3400
REP Fast	Cisco IOS XE 16.11.1	Initial support on Cisco Catalyst IE 3200, 3300, and 3400

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

168

VRRPv3 Protocol Support

VRRPv3 Protocol Support

Virtual Router Redundancy Protocol (VRRP) enables a group of devices to form a single virtual device to provide redundancy. The LAN clients can then be configured with the virtual device as their default gateway. The virtual device, representing a group of devices, is also known as a VRRP group. The VRRP version 3 (v3) Protocol Support feature provides the capability to support IPv4 and IPv6 addresses while VRRP version 2 (v2) only supports IPv4 addresses. This module explains concepts related to VRRPv3 and describes how to create and customize a VRRP group in a network. Benefits of using VRRPv3 Protocol Support include the following:

- Interoperability in multi-vendor environments.

- VRRPv3 supports usage of IPv4 and IPv6 addresses.

- Improved scalability through the use of VRRS Pathways.

Note   In this module, VRRP and VRRPv3 are used interchangeably.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfn.cloudapps.cisco.com/ITDIT/CFN/. An account on Cisco.com is not required.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

169

Restrictions for VRRPv3 Protocol Support

- VRRPv3 is not intended as a replacement for existing dynamic protocols. VRRPv3 is designed for use over multi-access, multicast, or broadcast capable Ethernet LANs.

- VRRPv3 is supported on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces and on VLANs.

- VRRPv3 does not support Stateful Switchover (SSO).

- Full network redundancy can only be achieved if VRRP operates over the same network path as the VRRS Pathway redundant interfaces. For full redundancy, the following restrictions apply:

  - VRRS pathways should not share a different physical interface as the parent VRRP group or be configured on a sub-interface having a different physical interface as the parent VRRP group.

  - VRRS pathways should not be configured on Switch Virtual Interface (SVI) interfaces as long as the associated VLAN does not share the same trunk as the VLAN on which the parent VRRP group is configured.

Information About VRRPv3 Protocol Support

VRRPv3 Benefits

Support for IPv4 and IPv6

VRRPv3 supports IPv4 and IPv6 address families.

Note   VRRPv2 is not supported. For VRRPv3 to be configurable, the **fhrp version vrrp v3** command must be used in global configuration mode

Redundancy

VRRP enables you to configure multiple devices as the default gateway device, which reduces the possibility of a single point of failure in a network.

Load Sharing

You can configure VRRP in such a way that traffic to and from LAN clients can be shared by multiple devices, thereby sharing the traffic load more equitably between available devices.

Multiple Virtual Devices

VRRP supports up to 32 virtual devices (VRRP groups) on a device physical interface, subject to restrictions in scaling. Multiple virtual device support enables you to implement redundancy and load sharing in your LAN topology. In scaled environments, VRRS Pathways should be used in combination with VRRP control groups.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

170

Multiple IP Addresses

The virtual device can manage multiple IP addresses, including secondary IP addresses. Therefore, if you have multiple subnets configured on an Ethernet interface, you can configure VRRP on each subnet.

Note   To utilize secondary IP addresses in a VRRP group, a primary address must be configured on the same group.

Preemption

The redundancy scheme of VRRP enables you to preempt a virtual device backup that has taken over for a failing virtual device master with a higher priority virtual device backup that has become available.

Note   Preemption of a lower priority master device is enabled with an optional delay.

Advertisement Protocol

VRRP uses a dedicated Internet Assigned Numbers Authority (IANA) standard multicast address for VRRP advertisements. For IPv4, the multicast address is 224.0.0.18. For IPv6, the multicast address is FF02:0:0:0:0:0:0:12. This addressing scheme minimizes the number of devices that must service the multicasts and allows test equipment to accurately identify VRRP packets on a segment. The IANA has assigned VRRP the IP protocol number 112.

VRRP Device Priority and Preemption

An important aspect of the VRRP redundancy scheme is VRRP device priority. Priority determines the role that each VRRP device plays and what happens if the virtual device master fails.

If a VRRP device owns the IP address of the virtual device and the IP address of the physical interface, this device will function as a virtual device master.

Priority also determines if a VRRP device functions as a virtual device backup and the order of ascendancy to becoming a virtual device master if the virtual device master fails. You can configure the priority of each virtual device backup with a value of 1 through 254 using the **priority** command (use the **vrrp address-family** command to enter the VRRP configuration mode and access the **priority** option).

For example, if device A, the virtual device master in a LAN topology, fails, an election process takes place to determine if virtual device backups B or C should take over. If devices B and C are configured with the priorities of 101 and 100, respectively, device B is elected to become virtual device master because it has the higher priority. If devices B and C are both configured with the priority of 100, the virtual device backup with the higher IP address is elected to become the virtual device master.

By default, a preemptive scheme is enabled whereby a higher priority virtual device backup that becomes available takes over from the virtual device backup that was elected to become virtual device master. You can disable this preemptive scheme using the **no preempt** command (use the **vrrp address-family** command to enter the VRRP configuration mode, and enter the **no preempt** command). If preemption is disabled, the virtual device backup that is elected to become virtual device master remains the master until the original virtual device master recovers and becomes master again.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches ◾

171

Note   Preemption of a lower priority master device is enabled with an optional delay.

VRRP Advertisements

The virtual device master sends VRRP advertisements to other VRRP devices in the same group. The advertisements communicate the priority and state of the virtual device master. The VRRP advertisements are encapsulated into either IPv4 or IPv6 packets (based on the VRRP group configuration) and sent to the appropriate multicast address assigned to the VRRP group. For IPv4, the multicast address is 224.0.0.18. For IPv6, the multicast address is FF02:0:0:0:0:0:0:12. The advertisements are sent every second by default and the interval is configurable.

Cisco devices allow you to configure millisecond timers. You need to manually configure the millisecond timer values on both the primary and the backup devices. The master advertisement value displayed in the **show vrrp** command output on the backup devices is always 1 second because the packets on the backup devices do not accept millisecond values.

You must use millisecond timers where absolutely necessary and with careful consideration and testing. Millisecond values work only under favorable circumstances. The use of the millisecond timer values is compatible with third party vendors, as long as they also support VRRPv3. You can specify a timer value between 100 milliseconds and 40000 milliseconds.

How to Configure VRRPv3 Protocol Support

Creating and Customizing a VRRP Group

To create a VRRP group, perform the following task. Steps 6 to 14 denote customizing options for the group, and they are optional:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **fhrp version vrrp v3**
4. **interface** *type number*
5. **vrrp** *group-id* **address-family** {**ipv4** | **ipv6**}
6. **address** *ip-address* [**primary** | **secondary**]
7. **description** *group-description*
8. **match-address**
9. **preempt delay minimum** *seconds*
10. **priority** *priority-level*
11. **timers advertise** *interval*
12. **vrrs leader** *vrrs-leader-name*
13. **shutdown**
14. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**fhrp version vrrp v3** **Example:** `Device(config)# fhrp version vrrp v3`	Enables the ability to configure VRRPv3 and VRRS.
Step 4	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 1/1`	Enters interface configuration mode.
Step 5	**vrrp** *group-id* **address-family** {**ipv4** | **ipv6**} **Example:** `Device(config-if)# vrrp 3 address-family ipv4`	Creates a VRRP group and enters VRRP configuration mode.
Step 6	**address** *ip-address* [**primary** | **secondary**] **Example:** `Device(config-if-vrrp)# address 100.0.1.10 primary`	Specifies a primary or secondary address for the VRRP group. **Note** VRRPv3 for IPv6 requires that a primary virtual link-local IPv6 address is configured to allow the group to operate. After the primary link-local IPv6 address is established on the group, you can add the secondary global addresses.
Step 7	**description** *group-description* **Example:** `Device(config-if-vrrp)# description group 3`	(Optional) Specifies a description for the VRRP group.
Step 8	**match-address** **Example:** `Device(config-if-vrrp)# match-address`	(Optional) Matches secondary address in the advertisement packet against the configured address. • Secondary address matching is enabled by default.
Step 9	**preempt delay minimum** *seconds* **Example:**	(Optional) Enables preemption of lower priority master device with an optional delay. • Preemption is enabled by default.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

173

	Command or Action	Purpose
	`Device(config-if-vrrp)# preempt delay minimum 30`	
Step 10	**priority** *priority-level* **Example:** `Device(config-if-vrrp)# priority 3`	(Optional) Specifies the priority value of the VRRP group. • The priority of a VRRP group is 100 by default.
Step 11	**timers advertise** *interval* **Example:** `Device(config-if-vrrp)# timers advertise 1000`	(Optional) Sets the advertisement timer in milliseconds. • The advertisement timer is set to 1000 milliseconds by default.
Step 12	**vrrs leader** *vrrs-leader-name* **Example:** `Device(config-if-vrrp)# vrrs leader leader-1`	(Optional) Specifies a leader's name to be registered with VRRS and to be used by followers. • A registered VRRS name is unavailable by default.
Step 13	**shutdown** **Example:** `Device(config-if-vrrp)# shutdown`	(Optional) Disables VRRP configuration for the VRRP group. • VRRP configuration is enabled for a VRRP group by default.
Step 14	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring the Delay Period Before FHRP Client Initialization

To configure the delay period before the initialization of all FHRP clients on an interface, perform the following task:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **fhrp version vrrp v3**
4. **interface** *type number*
5. **fhrp delay** {[**minimum**] [**reload**] *seconds*}
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

174

	Command or Action	Purpose
	Example: Device> enable	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**fhrp version vrrp v3** **Example:** Device(config)# fhrp version vrrp v3	Enables the ability to configure VRRPv3 and VRRS.
Step 4	**interface** *type number* **Example:** Device(config)# interface GigabitEthernet 1/1	Enters interface configuration mode.
Step 5	**fhrp delay** {[**minimum**] [**reload**] *seconds*} **Example:** Device(config-if)# fhrp delay minimum 5	Specifies the delay period for the initialization of FHRP clients after an interface comes up. • The range is 0-3600 seconds.
Step 6	**end** **Example:** Device(config)# end	Returns to privileged EXEC mode.

Configuration Examples for VRRPv3 Protocol Support

Example: Enabling VRRPv3 on a Device

The following example shows how to enable VRRPv3 on a device:

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config-if-vrrp)# end
```

Example: Creating and Customizing a VRRP Group

The following example shows how to create and customize a VRRP group:

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

175

```
Device(config)# interface GigabitEthernet 1/1
Device(config-if)# vrrp 3 address-family ipv4
Device(config-if-vrrp)# address 100.0.1.10 primary
Device(config-if-vrrp)# description group 3
Device(config-if-vrrp)# match-address
Device(config-if-vrrp)# preempt delay minimum 30
Device(config-if-vrrp)# end
```

Note   In the above example, the **fhrp version vrrp v3** command is used in the global configuration mode.

Example: Configuring the Delay Period Before FHRP Client Initialization

The following example shows how to configure the delay period before FHRP client initialization :

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config)# interface GigabitEthernet 1/1
Device(config-if)# fhrp delay minimum 5
Device(config-if-vrrp)# end
```

Note   In the above example, a five-second delay period is specified for the initialization of FHRP clients after the interface comes up. You can specify a delay period between 0 and 3600 seconds.

Example: VRRP Status, Configuration, and Statistics Details

The following is a sample output of the status, configuration and statistics details for a VRRP group:

```
Device> enable
Device# show vrrp detail

 GigabitEthernet1/1 - Group 3 - Address-Family IPv4
  Description is "group 3"
  State is MASTER
  State duration 53.901 secs
  Virtual IP address is 100.0.1.10
  Virtual MAC address is 0000.5E00.0103
  Advertisement interval is 1000 msec
  Preemption enabled, delay min 30 secs (0 msec remaining)
  Priority is 100
  Master Router is 10.21.0.1 (local), priority is 100
  Master Advertisement interval is 1000 msec (expires in 832 msec)
  Master Down interval is unknown
  VRRPv3 Advertisements: sent 61 (errors 0) - rcvd 0
  VRRPv2 Advertisements: sent 0 (errors 0) - rcvd 0
  Group Discarded Packets: 0
    VRRPv2 incompatibility: 0
    IP Address Owner conflicts: 0
    Invalid address count: 0
    IP address configuration mismatch : 0
    Invalid Advert Interval: 0
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

176

```
   Adverts received in Init state: 0
   Invalid group other reason: 0
 Group State transition:
   Init to master: 0
   Init to backup: 1 (Last change Sun Mar 13 19:52:56.874)
   Backup to master: 1 (Last change Sun Mar 13 19:53:00.484)
   Master to backup: 0
   Master to init: 0
   Backup to init: 0

Device# exit
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Commands List, All Releases
FHRP commands	First Hop Redundancy Protocols Command Reference
VRRPv3 Commands	For complete syntax and usage information for the commands used in this chapter.

Standards and RFCs

Standard/RFC	Title
RFC5798	*Virtual Router Redundancy Protocol*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Glossary

Virtual IP address owner—The VRRP device that owns the IP address of the virtual device. The owner is the device that has the virtual device address as its physical interface address.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

177

Virtual device—One or more VRRP devices that form a group. The virtual device acts as the default gateway device for LAN clients. The virtual device is also known as a VRRP group.

Virtual device backup—One or more VRRP devices that are available to assume the role of forwarding packets if the virtual device master fails.

Virtual device master—The VRRP device that is currently responsible for forwarding packets sent to the IP addresses of the virtual device. Usually, the virtual device master also functions as the IP address owner.

VRRP device—A device that is running VRRP.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

178

Device Level Ring

Device Level Ring

Device Level Ring (DLR) is a Layer 2 protocol that enables redundancy in a ring topology, providing fast network fault detection and reconfiguration for industrial networks. DLR is an EtherNet/IP™ protocol that is defined by the Open DeviceNet® Vendors' Association (ODVA).

DLR network includes at least one node configured to be a ring supervisor, and any number of normal ring nodes. All DLR ring nodes are required to have at least two Ethernet ports and incorporate embedded switch technology. Non-DLR multiport devices—switches or end devices—may be present in the ring, subject to certain implementation constraints. (No MAC table filtering is one example.) Non-DLR devices also affect the worst-case ring recovery time.

The DLR protocol supports a simple, single-ring topology. However, a network installation may use more than one DLR-based ring, so long as each ring is isolated so that DLR protocol messages from one ring are not present on another ring.

DLR supports redundant gateways for connecting with network infrastructure outside of the DLR network. The DLR redundant gateway feature provides mechanisms for automatically or manually selecting an active gateway. It also provides for automatic switchover to a backup gateway in the event of a connection failure.

A DLR ring can operate on access or trunk interfaces. A DLR ring configured with access ports can connect switches or end nodes. A DLR ring with trunk interfaces serves as an infrastructure that connects DLR-capable switches and devices in multiple VLANs. All the interfaces on the ring should have the same VLAN membership.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

179

Components of DLR

DLR Device Classes

DLR supports two classes of devices:

- *Ring supervisor*: On every DLR network, you must configure at least one device as the ring supervisor. The ring supervisor verifies the integrity of the ring, reconfigures it when a fault occurs, and collects diagnostic information. The ring supervisor also sends and processes Beacon frames at the default beacon interval of 400 microseconds.

  We recommend that you make at least one other device on the DLR network available as a back-up ring supervisor. Each supervisor is configured with a precedence value; the device with the highest precedence value becomes the active ring supervisor.

- *Beacon-based ring node*: This class of device implements the DLR protocol, but lacks ring supervisor capability. The device must be able to process and act on the beacon frames that the ring supervisor sends.

Redundant Gateway

In a DLR network, redundant gateway devices enable multiple connections to the network outside of the DLR network. They provide an alternate path for communication in case a gateway device or its connection to the outside network fails.

For information about redundant gateways, see the sections Redundant Gateways, on page 185 and Configure a Redundant Gateway, on page 194 in this guide.

Default and Redundancy FPGA Profiles

Because the DLR feature requires use of the IE3400 switch FPGA, the number of DLR rings supported on the IE3400 depends on the FPGA profile. The default FPGA profile supports only one DLR ring on the base system. For additional DLR rings on the IE3400 base system, you must change the FPGA profile from the default to the Redundancy profile. When the FPGA's redundancy profile is active, the IE3400 base system supports two DLR rings.

The same limitations exist for IE3400 expansion modules. IE3400 expansion modules have product ID prefix *IEM-3400*. The eight-port IEM-3400 expansion modules support one DLR ring default FPGA profile; they support two DLR rings in redundancy profile. When a IE3400 switch has one eight-port IEM-3400 expansion module, it supports two DLR rings—one with interfaces terminating on the base system, and the other with interfaces terminating on the expansion module. To achieve three DLR rings, the IE3400 switch must have the redundancy FPGA profile configured.

The switch can support a maximum of three DLR rings. To have three rings, configure a redundancy profile in which one DLR ring is on the base card and two rings are on the expansion card. Or, you can configure two rings on the base card and one ring on the expansion line card.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

180

DLR Topology

A Cisco Catalyst IE3400 Rugged Series Switch can act as a DLR ring supervisor, backup supervisor, or regular DLR beacon node. This functionality helps other nodes that are connected in a DLR with Cisco Catalyst IE3400 Rugged Series Switches to recover from a ring fault within 3 milliseconds and resume communications.

The following illustration shows a DLR ring with Cisco Catalyst IE3400 Rugged Series Switches acting as the ring supervisor, backup supervisor, and beacon nodes. The solid blue line represents the ring over which Ethernet frames travel, and the dotted gray line represents the bidirectional beacon frames. The X in the illustration shows where the ring supervisor blocks an interface to prevent broadcast storms. If a failure occurs in the DLR ring, the supervisor will unblock the interface.

Figure 24: DLR Topology
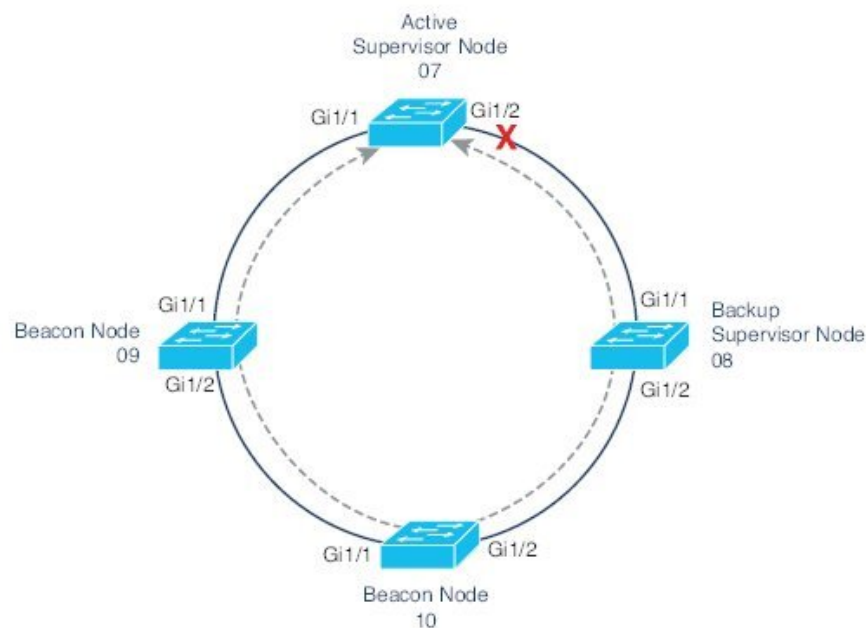
We recommend that you connect the interface with the higher number on the active supervisor node to the backup supervisor node.

Multiple Rings

Cisco Catalyst IE3400 Rugged Series Switches and Cisco Catalyst IE3400 Heavy-Duty Series Switches support up to three rings.

Multiple Rings, Single Switch, Single VLAN

The following restrictions apply to multiple rings that are connected to one switch on one VLAN:

- Multiple rings cannot share the same ring ports.
- Ring ports function only as access ports.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

181

- All ports participating in the ring must have the same VLAN mode. If an access ring is configured, then all ports must be in the same access VLAN. For a trunk ring, all ports must be in trunk mode.

When only one node is a member of multiple rings, as in the example below, a VLAN can have ports in more than one ring.

Figure 25: Multiple Rings, Single Switch, Single VLAN
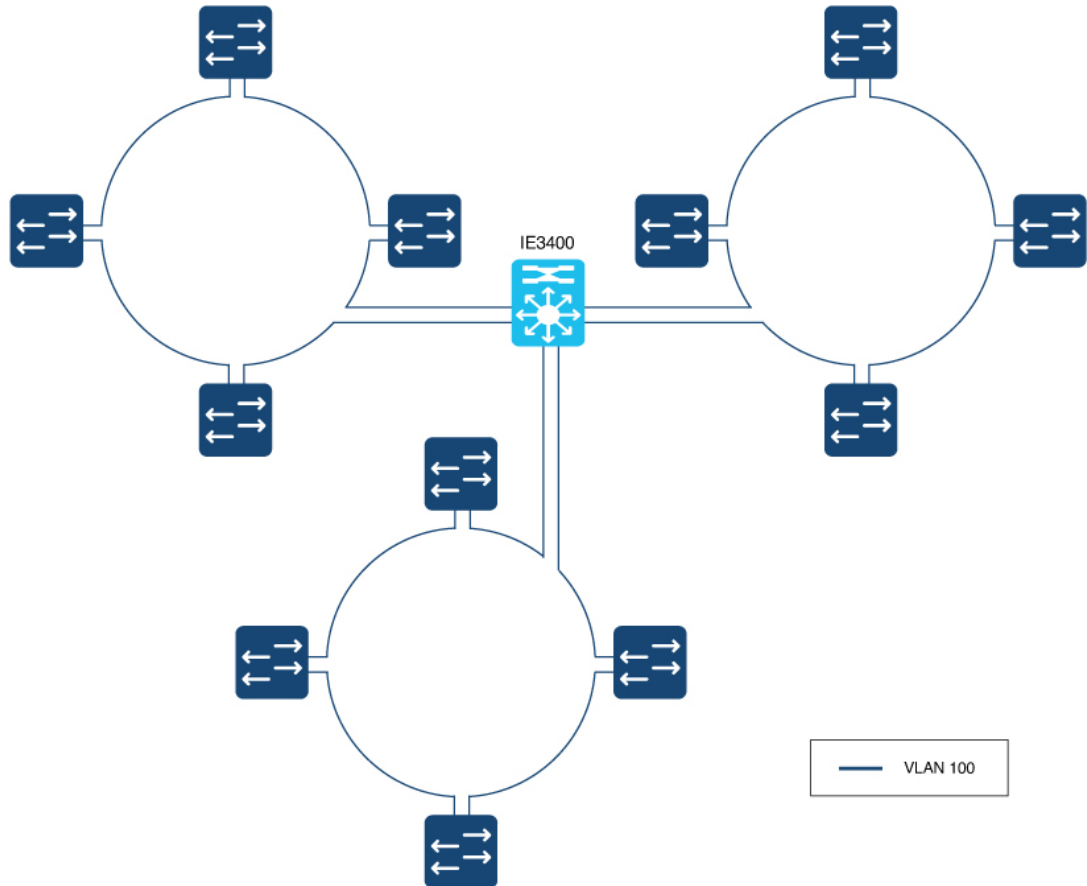
Multiple Rings, Single Switch, Multiple VLANs

The following illustration shows multiple rings sharing a common supervisor with unique VLANs for each ring. When each DLR ring operates in a different VLAN, there is no issue and this is a supported deployment.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

182

Figure 26: Multiple Rings, Single Switch, Multiple VLANs
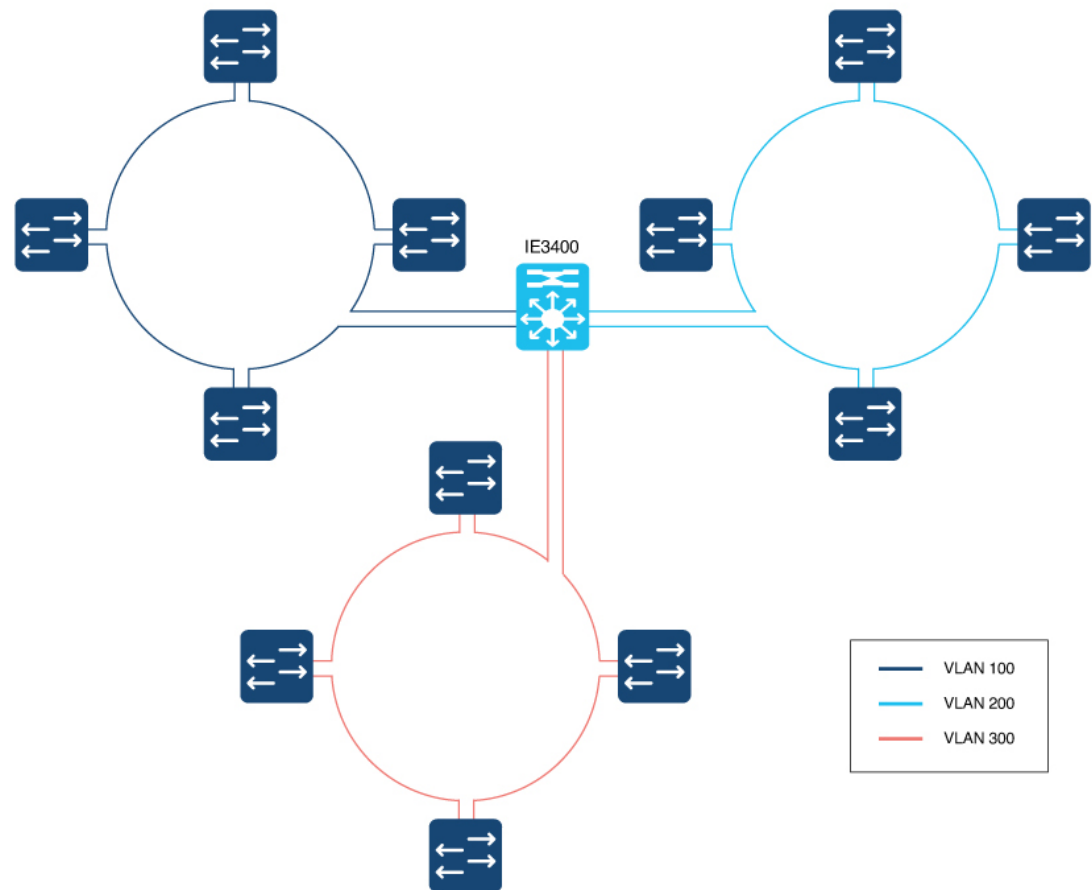
Multiple Rings Connected to Multiple Switches

You can also use multiple rings with multiple IE3400 switches, as shown in the illustration below. Depending on the configuration of the switches, VLAN restrictions can apply.

If the two switches are configured as redundant gateways for the same set of rings, there are no VLAN restrictions. The following example shows two rings on the same VLAN and one ring on a separate VLAN. However, because there are no VLAN restrictions, you can also configure all three rings on the same VLAN or all three on separate VLANs.

When there are two or more switches in same DLR, and they are not configured as redundant gateways, then each DLR ring must have a unique VLAN. VLANs and mutiple DLR rings need to be planned, especially when the VLAN or VLANs are present on more than one DLR ring. Configuring redundant gateways on the IE switches enables DLR deployments where a VLAN is present on multiple DLR rings. When the DLR gateway is not configured on the IE switch pair, then a VLAN cannot be shared across rings. Failure to adhere to this guidance will result in a Layer 2 loop. In example below, the two IE switches are configured for DLR gateway, thus a VLAN can be present across two or more DLR rings.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches ■

183

Figure 27: Multiple Rings, Multiple Switches, No VLAN Restrictions
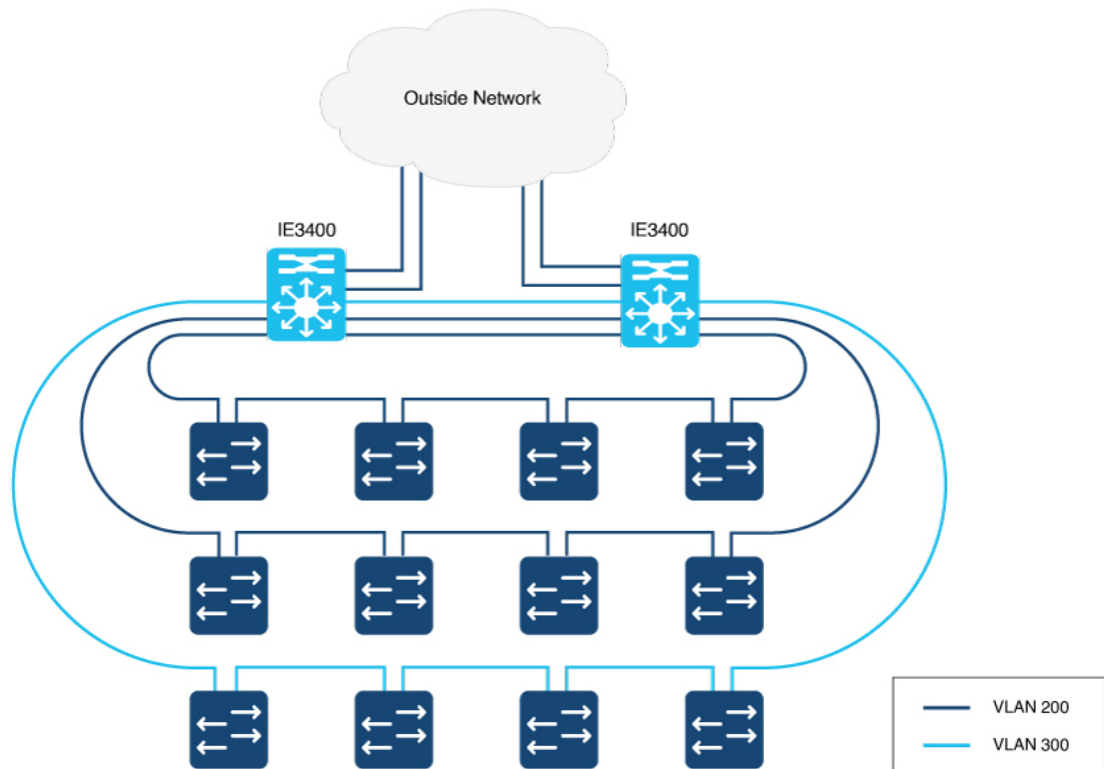
If the two switches are not configured as redundant gateways, VLANs cannot be present on more than one ring, otherwise a Layer 2 loop becomes possible. The following illustration shows only one path out of the DLR ring, so DLR redundant gateways have not been configured.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

184

Figure 28: Vlans Not Shared Across DLR Rings
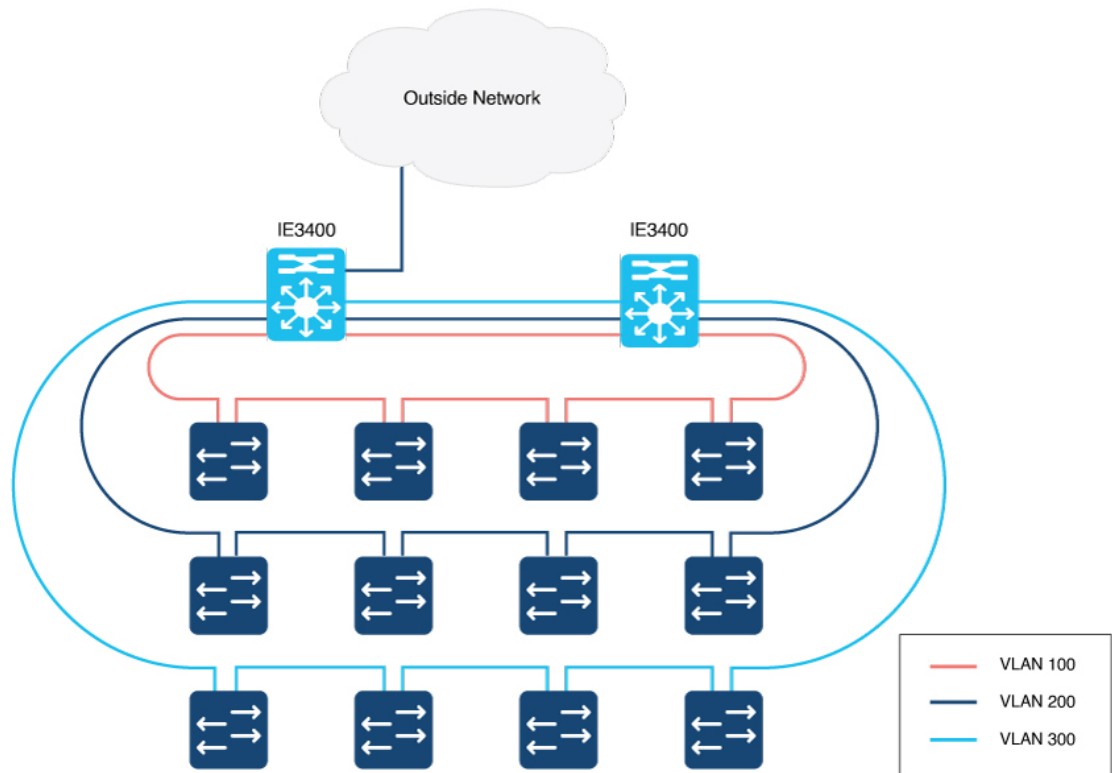
Redundant Gateways

A DLR network with redundant gateways uses multiple switches to provide multiple connections from a ring to the outside network. Redundant gateways are not essential if you need only one connection to the outside network, but they provide extra network resiliency if an uplink connection fails.

Either a ring supervisor or a ring participant can be a redundant gateway; however, you must enable and configure DLR on both gateway switches.

Redundant gateways enable you to automatically or manually chose an active gateway as well as for automatic switchover to a backup gateway in case of a connection failure. Gateway switchover times range from 14 ms to 6.1 seconds, depending on the uplink network resiliency protocol. DLR redundancy gateway performance applies to traffic sourced from inside the DLR destined to the outside network:

- Uplink connection failure detected by the active gateway at the physical layer is anywhere from 14 to 150 ms.

- Failure of the Active Gateway Node can take between 19 and 150 ms.

System performance, which applies to most applications, describes traffic sourced from the outside network destined to the DLR. Higher layer uplink fault detection is up to 6.1 seconds.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

185

DLR gateway convergence depends on the redundancy protocol running on the gateway interfaces. STP and REP have different convergence times. Traffic in and out of the DLR ring to the outside network should converge on failure to match the protocol used.

The following illustration shows traffic flow in and out of a DLR ring through the active DLR gateway.

Figure 29: DLR Active Gateway Traffic Flow
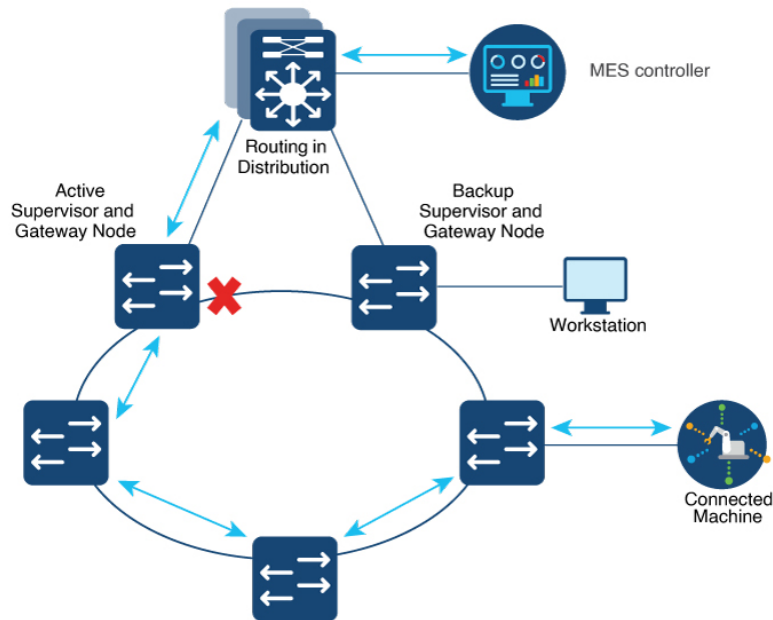
The following illustration shows traffic flow in and out of a DLR ring through the backup DLR gateway for devices directly connected to the backup gateway node. It is important to understand the physical path devices take to communicate with other applications outside the ring. The devices attached to the configured backup gateway take a different path than devices attached to the active gateway or other nodes in the DLR ring.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

186

Figure 30: DLR Backup Gateway Traffic Flow
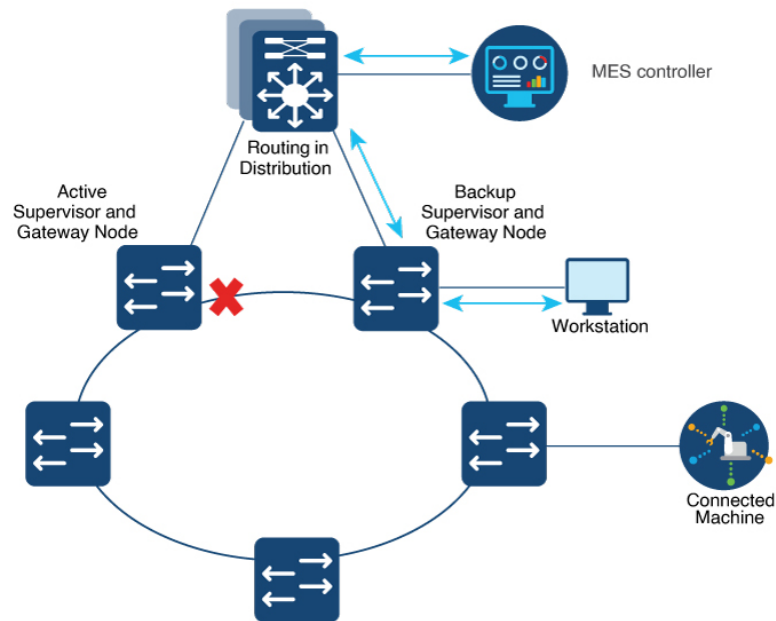
For more information about redundant gateways, see *Guidelines for Using Device Level Ring (DLR) with Ethernet/IP*™ on the odva.org website.

Cisco IE Switch Support for DLR

Cisco Catalyst IE3400 Rugged Series Switches and Cisco Catalyst IE3400 Heavy-Duty Series Switches support DLR beginning with the Cisco IOS XE Dublin 17.11.1 Release.

Switches that Support DLR

The following switches support DLR:

- Cisco Catalyst IE3400 Rugged Series Switches

    - IE3400-8P2S

    - IE3400-8T2S

- Cisco Catalyst IE3400 Heavy-Duty Series Switches (All versions0

Support for DLR is available on Network Essentials and Network Advantage licenses.

Supported DLR Features

IE3400-8P2S, IE3400-8T2S, and IE3400 Heavy Duty Switches support the following DLR features:

- Three DLR rings for each switch and expansion model combination as shown in the following table.

    When using the default FPGA profile, an IE3400 Rugged Series switch with an IEM-3400 expansion module supports no more than two rings. An IE3400 Rugged Series base switch supports only one DLR

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches ■

187

ring when using the default FPGA profile. The following table shows the number of rings that each IE3400 switch and expansion model support.

Switch	FPGA Profile	Number of Rings
IE3400 Rugged Series without expansion module	Default	1
	Redundancy	2
IE3400 Rugged Series with expansion module	Default	2 One ring on base switch ports and 1 ring on expansion module ports
	Redundancy	3 • Two rings on base switch ports and one ring on expansion module ports • One ring on base switch ports and 2 rings on expansion module ports
IE3400 Heavy-Duty series with 8 ports (1 FPGA)	Default	1
	Redundancy	2
IE3400 Heavy-Duty series with 16 or 24 ports (2 or 3 FPGAs)	Default	2 One ring on base module ports (Gi1/1-8) and 1 ring on expansion module ports (Gi1/9-16)
	Redundancy	3 • 2 rings on the base switch (Gi1/1-8) and 1 ring on expansion module ports • One ring on the base switch (Gi1/1-8) and 2 rings on the expansion module (Gi1/9-16)

• Redundant gateway

• Web User Interface (WebUI): DLR can be configured using the WebUI.

• Common Industrial Protocol (CIP): DLR can be configured using CIP.

Differences Between Switch Models When Using DLR

Port mapping for IE3400 Heavy-Duty Series Switches differs from port mapping for IE3400-8P2S and IE3400-8T2S Rugged Series Switches.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

188

For IE3400-8P2S and IE3400-8T2S Rugged Series Switches, DLR is supported on all ports on the base system Gi1/1 through Gi1/10, and on the expansion module Gi2/1 through Gi2/8. DLR is supported on any adjacent port pair (N, N+1), where N is an odd port number.

The following table provides examples of the ports that you can use for each ring.

Table 3: Examples of IE3400 Rugged Series Switch Port Mapping

Ring 1		Ring 2		Ring 3	
Port 1	Port 2	Port 1	Port 2	Port 1	Port 2
Gig1/3, Gig1/5	Gig1/4, Gig1/6	Gig1/7, Gig1/9	Gig1/8, Gig1/10	Gig2/3, Gig2/5	Gig2/4, Gig2/6
Gig1/3,Gig1/5	Gig1/4, Gig1/6	Gig2/1, Gig2/3	Gig2/2, Gig2/4	Gig2/5,Gig2/7	Gig2/6, Gig2/8

For IE3400 Heavy-Duty Series Switches, each set of 8 ports supports a single DLR ring. Gi1/1 through Gi1/8 is one set, and Gi1/9 through Gi1/6 is a second set of ports. For IE3400 Rugged Series Switches (with eight, 16, or 24 ports), DLR is supported on Ports Gig1/1 through Gig1/16. Ports Gi1/17 through Gi1/24 do not support DLR.

For IE3400 Heavy-Duty Switches, you must pair DLR ring ports with adjacent ports. The following table shows valid DLR ring port pairs:

Table 4: IE3400 Heavy-Duty Switch Port Pairing

Ports	Valid DLR Ring Port Pairs
Gi1/1 through Gi1/8	• [Gi1/1, Gi1/2] • [Gi1/3, Gi1/4] • [Gi1/5, Gi1/6] • [Gi1/7, Gi1/8]
Gi1/9 through Gi1/16	• [Gi1/9, Gi1/10] • [Gi1/11, Gi1/12] • [Gi1/13, Gi1/14] • [Gi1/15, Gi1/16]

When using the default FPGA profile, you can have one ring on ports Gi1/1 trough Gi1/8, and one ring on ports Gi1/9 through Gi1/16, if available. When using the redundancy FPGA profile, you can have one or two rings on Gi1/1 through Gi1/8 and one or two rings on Gi1/9 through Gi1/16, if available. Regardless of the profile, you cannot have a ring on ports Gi1/17 through Gi1/24.

Note   You cannot form a ring with ports from different line cards.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

189

DLR Feature Interactions

The following list contains features that cannot be configured on interfaces that are also configured as DLR ring ports..

- STP, RSTP, and MSTP

- 802.1x and Guest VLAN

- PVLAN and PVLAN Edge

- VLAN Routing and Bridging and MV

DLR does not interfere with the functionality of the following features. However, take care during configuration: The MAC or IP addresses of the DLR devices must be included in the allowable list.

- Port Security

- Unicast MAC filter

- DAI

- DHCP Snooping

For the following features, the ports forward IGMP packets between the two DLR ports but do not process them. Devices other than gateways and active redundant gateway devices are unaffected.

- Multicast

- IGMP Snooping

Guidelines and Limitations

The following restrictions apply to DLR configuration and operation:

- You can configure up to three DLR rings at the same time on each Cisco Catalyst IE3400 Rugged Series Switch. See use cases in Multiple Rings, on page 181 for guidance.

- When configuring DLR Gateways, for each node, you can configure two ports as an uplink. An uplink can belong to more than one ring.

- We recommend that you configure no more than one backup gateway for each ring.

- MAC learning for each ring is limited to 1024 unicast MAC addresses and 128 multicast MAC addresses for each Cisco Catalyst IE3400 Rugged Series Switches.

- Multicast MAC learning through IGMP snooping is limited to 128 addresses.

- Duplicated packets may be observed during ring convergence.

- DLR is supported on 1 Gbps links and 100 Mbps interfaces with full duplex capability. DLR does not support half duplex links.

- PTP over DLR is supported in Cisco IOS XE Release 17.13.1 and later.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

190

- On a given physical ring, all the nodes must be configured with same ring- ID If there is any mismatch in ring IDs between nodes (due to misconfiguration), the ring will still converge and may lead to unexpected behavior.

The following restrictions apply to configuring multiple DLR rings:

- Multiple rings cannot share the same ring ports.

- The switch cannot be configured as announce-based node.

- The default beacon interval is 400 usec. This is the recommended interval for 1 Gbps and 100 Mbps ring interface speeds. The default beacon timeout is 1960 usec. This is the recommended value.

- DLR ring ports are supported on IEM-3400 expansion modules. DLR ring ports are not supported on IEM-3300 expansion modules. Check the Product ID (PID) of any expansion modules attached to the IE3400 before attempting to configure DLR rings on expansion module ports.

Note For information, including limitations, on DLR interactions with other features and protocols, see the section DLR Feature Interactions, on page 190 in this guide.

Configuring DLR

The following sections provide information for configuring DLR on Cisco Catalyst IE3400 Rugged Series Switches. The supervisor node with the highest precedence value is elected to operate as DLR supervisor. You can use this feature to plan which node will be active and which will be backup supervisor.

Configure a Ring Supervisor

Complete the following procedure to configure the switch as a ring supervisor.

Before you begin

Refer to the parameters for configuring a DLR ring supervisor, which are shown in the following table.

Parameter	Range	Default
Beacon interval	200 to100,000 microseconds	400 microseconds
Beacon timeout	200 to 500,000 microseconds	1960 microseconds
Precedence	0 to 255	0
control-vlan-id	0 to 4095	0

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches ■

■ **191**

Procedure

	Command or Action	Purpose
Step 1	**dlr ring** *ring_number* **Example:** switch(config)#dlr ring 1	Provide the unique DLR value identifying a ring.
Step 2	**mode** *device_role* **Example:** switch(config)#mode supervisor	Configure the DLR device as a ring supervisor.
Step 3	**beacon-interval** *microseconds* **Example:** switch(config)#beacon-interval 500	Set the beacon interval. **Note** You can set the beacon interval only for devices in supervisor mode.
Step 4	**beacon-timeout** *microseconds* **Example:** switch(config)# beacon-timeout 2500	Set the beacon timeout. **Note** You can set the beacon timeout only for devices in supervisor mode.
Step 5	**precedence** *rank* **Example:** switch(config)#precedence 100	Sets the precedence of the ring supervisor.
Step 6	**interface** *interface_name* **Example:** switch(config)#interface gigabitEthernet 1/3	Enter interface configuation submode for interface GigabitEthernet 1/3.
Step 7	**switchport mode access** **Example:** switch(config-if)#switchport mode access switch(config-if)#switchport access vlan 33	Configure the interface to be a member of a single VLAN.
Step 8	**dlr ring 1** **Example:** switch(config-if)#dlr ring 1	Configure the interface to be a member of a DLR ring.
Step 9	**interface** **Example:** switch(config)#interface gigabitEthernet 1/4	Set the interface for the second DLR ring port. The second DLR ring port must be a valid port pair of the first DLR ring port. See the section Cisco IE Switch Support for DLR, on page 187 in this guide for valid port pair combinations.
Step 10	**switchport mode access** **Example:** switch(config-if)#switchport mode access switch(config-if)#switchport access vlan 33	Configure the interface to be a member of a single VLAN. The VLAN must be the same as the one used by the other interface to be a port on same DLR ring.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

192

	Command or Action	Purpose
Step 11	**dlr ring 1** **Example:** `switch(config-if)#dlr ring 1`	Add interface for the DLR ring port.

What to do next

Verify that the ring supervisor is configured by entering the show command. The following example is output of the show command when the switch is configured as a ring supervisor:

```
Switch#sh dlr ring 1
DLR ring 1

mode: Active Supervisor
Network Topology:     Ring Network Status: Normal
IOS state: NORMAL_ACTIVE    Hardware State: NORMAL_ACTIVE
Transition bit = 0
Mac-Addr: 6C:13:D5:AC:3A:C3 IP-Addr: 0.0.0.0
Port1: GigabitEthernet1/3, vlan 33,   UP Port2: GigabitEthernet1/4, vlan 33, UP
LastBcnRcvPort: Port 1: Yes    Port 2: Yes

Active Supervisor Parameters:
Beacon Interval (usec): 500    Beacon Timeout (usec): 2500
DLR VLAN ID: 0       Precedence: 100
Mac-Addr: 6C:13:D5:AC:3A:C3    IP-Addr: 0.0.0.0

Locally Configured Supervisor Parameters:
Beacon Interval (usec): 500    Beacon Timeout (usec): 2500
DLR VLAN ID: 0       Precedence: 100
Port1: GigabitEthernet1/3    Port2: GigabitEthernet1/4
```

Configure a Beacon-Based Ring Node

Complete the commands as shown in the following example to configure the switch as a beacon-based ring node.

Example:

```
…
dlr ring 2
   mode beacon-node
!
…
interface GigabitEthernet1/1
   switchport mode trunk
   dlr ring 2
!
interface GigabitEthernet1/2
   switchport mode trunk
   dlr ring 2
!
…
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches ▮

▮ **193**

What to do next

Verify that the beacon-based ring node is configured by entering the show command. The following example is output of the show command when the switch is configured as a beacon-based ring node:

```
Switch#show dlr ring 2
DLR ring 2
mode: Beacon Node
Network Topology: Ring     Network Status: Normal
IOS state: NORMAL     Hardware State: NORMAL
Transition bit = 0
Mac-Addr: 6C:13:D5:AC:3C:03 IP-Addr: 0.0.0.0
Port1: GigabitEthernet1/1, vlan Trunk, UP  Port2: GigabitEthernet1/2, vlan Trunk, UP
LastBcnRcvPort: Port 1: Yes     Port 2: Yes

Active Supervisor Parameters:
Beacon Interval (usec): 400     Beacon Timeout (usec): 1960
DLR VLAN ID: 0 Precedence: 0
Mac-Addr: 6C:13:D5:AC:3A:C3     IP-Addr: 0.0.0.0

Locally Configured Beacon Node Parameters:
Port1: GigabitEthernet1/1    Port2: GigabitEthernet1/2
```

Configure a Redundant Gateway

You must configure DLR on both gateway switches.

Before you begin

Refer to the parameters for configuring a switch as a DLR redundant gateway node. The parameters are shown in the following table:

Parameter	Range	Default
Gateway enable	Enable-Disable	Disable
Precedence	0 to 255	0
Advertise interval	200 to 100,000 microseconds	2000 microseconds
Advertise timeout	500 to 500,000 microseconds	5000 microseconds
Learning-update	Supported	Enabled

Complete the commands as shown in the following example to configure the switch as a redundant gateway node.

Example:

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

194

Switch A Configuration	Switch B Configuration

…
dlr ring 1
 mode supervisor
dlr ring 1
 gateway enable
  gateway-precedence 100
  advertise-interval 3000
  advertise-timeout 10000
 	
interface GigabitEthernet1/9
 switchport mode trunk
 dlr ring 1 uplink
!…
	…
	dlr ring 1
	 mode supervisor
	dlr ring 1
	 gateway enable
	  gateway-precedence 255
	  advertise-interval 3000
	  advertise-timeout 10000
	
	interface GigabitEthernet1/9
	 switch mode trunk
	 dlr ring 1 uplink
	!…

What to do next

Verify that the redundant gateways are configured by entering the show command.

The following example is output of the show command when a switch is configured as the redundant gateway nodes:

```
Switch-a#sh dlr ring 1
DLR ring 1

mode: Active Supervisor
Network Topology: Ring     Network Status: Normal
IOS state: NORMAL_ACTIVE    Hardware State: NORMAL_ACTIVE
Transition bit = 0
Mac-Addr: 6C:13:D5:AC:3C:03 IP-Addr: 0.0.0.0
Port1: GigabitEthernet1/3, vlan Trunk, UP Port2: GigabitEthernet1/4, vlan Trunk, UP
LastBcnRcvPort: Port 1: Yes    Port 2: Yes

Active Supervisor Parameters:
Beacon Interval (usec): 400    Beacon Timeout (usec): 1960
DLR VLAN ID: 0      Precedence: 0
Mac-Addr: 6C:13:D5:AC:3C:03 IP-Addr: 0.0.0.0

Locally Configured Supervisor Parameters:
Beacon Interval (usec): 400    Beacon Timeout (usec): 1960
DLR VLAN ID: 0      Precedence: 0
Port1: GigabitEthernet1/3   Port2: GigabitEthernet1/4
…
…
…
Redundant Gateway Information:
Redundant Gateway Status: Active Gateway
Hardware State: ACTIVE NORMAL
Mac-Addr: 6C:13:D5:AC:3C:03 IP_addr:0.0.0.0
Uplink Port(s): GigabitEthernet1/9

Active Gateway Parameters:
Advertise Interval (usec): 3000  Advertise Timeout (usec): 10000
Precedence: 100    Learning Update Enable: yes
Mac-Addr: 6C:13:D5:AC:3C:03 IP-Addr:0.0.0.0

Fault Statistics:
Gateway Faults since power up: 0
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches ■

195

```
Locally Configured Gateway Parameters:
Advertise Interval (usec): 3000  Advertise Timeout (usec): 10000
Precedence: 100    Learning Update Enable: yes
Uplink Port(s): GigabitEthernet1/9
switch-a#
```

The following example is output of the show command when a switch is configured as the backup gateway:

```
Switch-b#sh dlr ring 1
-----------------------------------------
DLR ring 1

mode: Backup Supervisor
Network Topology: Ring    Network Status: Normal
IOS state: NORMAL_BACKUP   Hardware State: NORMAL_BACKUP
Transition bit = 0
Mac-Addr: 6C:13:D5:AC:3A:C3 IP-Addr: 0.0.0.0
Port1: GigabitEthernet1/3, vlan Trunk, UP Port2: GigabitEthernet1/4, vlan Trunk, UP
LastBcnRcvPort: Port 1:   Yes Port 2: Yes

Active Supervisor Parameters:
Beacon Interval (usec): 400   Beacon Timeout (usec): 1960
DLR VLAN ID: 0     Precedence: 0
Mac-Addr: 6C:13:D5:AC:3C:03 IP-Addr: 0.0.0.0

Locally Configured Supervisor Parameters:
Beacon Interval (usec): 400   Beacon Timeout (usec): 1960
DLR VLAN ID: 0     Precedence: 0
Port1: GigabitEthernet1/3   Port2: GigabitEthernet1/4
…
…
…
Backup Supervisor Precedence: 0

Redundant Gateway Information:
Redundant Gateway Status: Backup Gateway
Hardware State: BACKUP NORMAL
Mac-Addr: 6C:13:D5:AC:3A:C3 IP_addr:0.0.0.0
Uplink Port(s): GigabitEthernet1/1

Active Gateway Parameters:
Advertise Interval (usec): 3000  Advertise Timeout (usec): 10000
Precedence: 100    Learning Update Enable: yes
Mac-Addr: 6C:13:D5:AC:3C:03 IP-Addr:0.0.0.0

Fault Statistics:
Gateway Faults since power up: 0

Locally Configured Gateway Parameters:
Advertise Interval (usec): 3000  Advertise Timeout (usec): 10000
Precedence: 0     Learning Update Enable: yes
Uplink Port(s): GigabitEthernet1/1
```

Configure VLAN Trunking

Note	When a node has two or more DLR rings configured, a VLAN can only be present on one ring. When configuring DLR ring ports in trunk mode, you must edit the trunk-allowed VLAN list to ensure unique VLAN membership across DLR rings.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

196

Complete the commands as shown in the following example to configure VLAN trunking for DLR.

Example:

```
switch(config)#dlr ring 1
switch(config-dlr)#mode supervisor
switch(config-dlr-supervisor)#end

switch(config)#int gi1/3
switch(config-if)#switchport mode trunk
switch(config-if)#switchport trunk allowed vlan 10,20
switch(config-if)#dlr ring 1

switch(config-if)#
switch(config-if)#int gi1/4
switch(config-if)#switchport mode trunk
switch(config-if)#switchport trunk allowed vlan 10,20
switch(config-if)#dlr ring 1
```

What to do next

Verify that VLAN trunking is configured by entering the show command. The following example is the output of the show command when VLAN trunking is configured:

```
switch#sh dlr ring
----------------------------------------
DLR ring 1

mode: Active Supervisor
Network Topology: Ring      Network Status: Normal
IOS state: NORMAL_ACTIVE     Hardware State: NORMAL_ACTIVE
Transition bit = 0
Mac-Addr: 6C:13:D5:AC:3A:C3 IP-Addr: 0.0.0.0
Port1: GigabitEthernet1/3, vlan Trunk, UP  Port2: GigabitEthernet1/4, vlan Trunk, UP
LastBcnRcvPort: Port 1: Yes    Port 2: Yes

Active Supervisor Parameters:
Beacon Interval (usec): 400    Beacon Timeout (usec): 1960
DLR VLAN ID: 0      Precedence: 0
Mac-Addr: 6C:13:D5:AC:3A:C3 IP-Addr: 0.0.0.0

Locally Configured Supervisor Parameters:
Beacon Interval (usec): 400    Beacon Timeout (usec): 1960
DLR VLAN ID: 0      Precedence: 0
Port1: GigabitEthernet1/3    Port2: GigabitEthernet1/4

Ring Protocol Participants Count: 3
No    Mac-Addr IP-Addr
1     6C:13:D5:AC:3A:C3 0.0.0.0
2     6C:13:D5:AC:3C:03 0.0.0.0
3     6C:13:D5:AC:37:03 0.0.0.0

Fault Statistics:CIP

Ring Faults since power up: 0
Ring Fault Location  Mac-Addr IP-Addr
Last Active Node on Port 1 00:00:00:00:00:000.0.0.0
Last Active Node on Port 2 00:00:00:00:00:000.0.0.0

Redundant Gateway Information:
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

197

```
Redundant Gateway Status: Gateway not enabled
---------------------------------------
DLR ring 2 not configured
```

Enabling CIP

You can enable Common Industrial Protocol (CIP) on a device by applying the `cip enable` command on one of the Layer-3 interfaces—a physical L3 interface or an SVI-interface.

> **Note**   Be aware of the following when enabling CIP:
>
> • You must habve DLR rings configured on the switch before enabling CIP.
>
> • You must enter the command in interface configuration mode.
>
> • You enable CIP at the device level.
>
> • You enable CIP only through one of the Layer-3 interfaces; if you try to enable CIP on another interface, an error occurs.

Enable CIP on the Layer 3 Interface

Complete the steps in this section to enable CIP on the Layer 3 interface.

Procedure

	Command or Action	Purpose
Step 1	**conf t**	Enter configuration mode.
Step 2	**interface** *interface_name* **Example:** `switch(config)#interface gigabitEthernet 1/10`	Specify the interface.
Step 3	**no switchport**	Prevent the interface from forwarding Ethernet frames based on MAC addresses. The interface is not operational until a valid IP address is assigned.

Step 4	**ip address** *IP_address subnet_address*
	
	Example:
	`switch(config-if)#ip address 192.168.1.10`
	`255.255.255.0`
		Set the IP address and subnet.

Step 5	**cip enable**	Enable CIP on the interface.
Step 6	**end**	Leave configuration mode.

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

198

What to do next

Verify that CIP is configured by entering the show command. The following example is output of the `show` command when CIP is configured:

```
DLR_node#show cip status
State : Enabled
Interface : Gi1/10
DLR_node#
```

Enable CIP on the SVI Interface

Complete the steps in this section to enable CIP on the SVI interface.

Before you begin

If the SVI is not vlan1, assign `switchport access vlan` *vlan-id* to the DLR ring.

Procedure

	Command or Action	Purpose
Step 1	**conf t**	Enter configuration mode.
Step 2	**vlan** *vlan_id* **Example:** `switch(config)#vlan 1`	Specify the VLAN.
Step 3	int vlan *vlan_id* **Example:** `switch(config-vlan)#int vlan 1`	Enter interface configuration mode.

Step 4	**ip address** *IP_address subnet_address*
	
	Example:
	`switch(config-if)#ip address 192.168.1.10`
	`255.255.255.0`
		Specify an ID address and subnet.

Step 5	**cip enable** **Example:** `switch(config-if)# cip enable`	Enable CIP on the interface.
Step 6	**end** **Example:** `switch(config-if)# end`	Leave configuration mode.

What to do next

Verify that CIP is configured by entering the show command. The following example is output of the `show` command when CIP is configured:

```
DLR_node#show cip status
State : Enabled
```

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

199

```
Interface : Vlan 1
DLR_node#
```

Feature History

The following table shows the Cisco IOS release in which the feature is first supported on each of the IE switch platforms that support Device Level Ring.

Switch Platform	Feature	Initial Release
• Cisco Catalyst IE3400 Rugged Series Switches • Cisco Catalyst IE3400 Heavy Duty Series Switches	Device Level Ring	Cisco IOS XE Dublin 17.11.1

Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches

200