Redundancy Protocol Configuration Guide, Cisco Catalyst IE31xx Series Switches

First Published: 2020-08-10

Last Modified: 2025-04-25

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

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

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

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

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

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

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

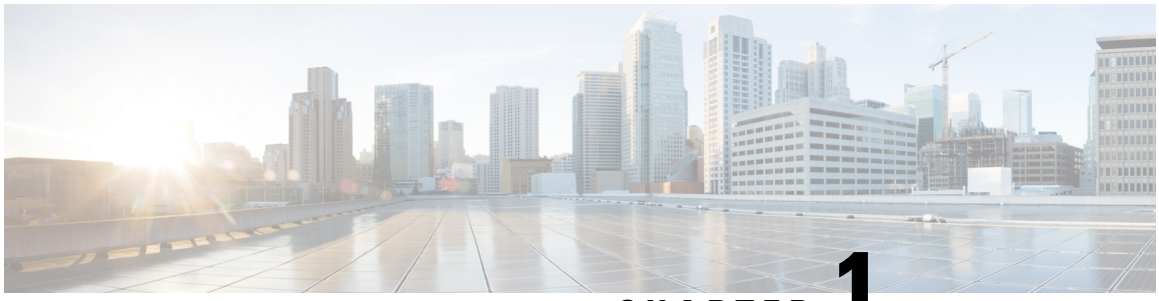
All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

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

© 2020–2025 Cisco Systems, Inc. All rights reserved.

CONTENTS



CHAPTER 1

Media Redundancy Protocol

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: 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 IE3100 switches:

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

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

All MRM and MRC ring ports support the following states:

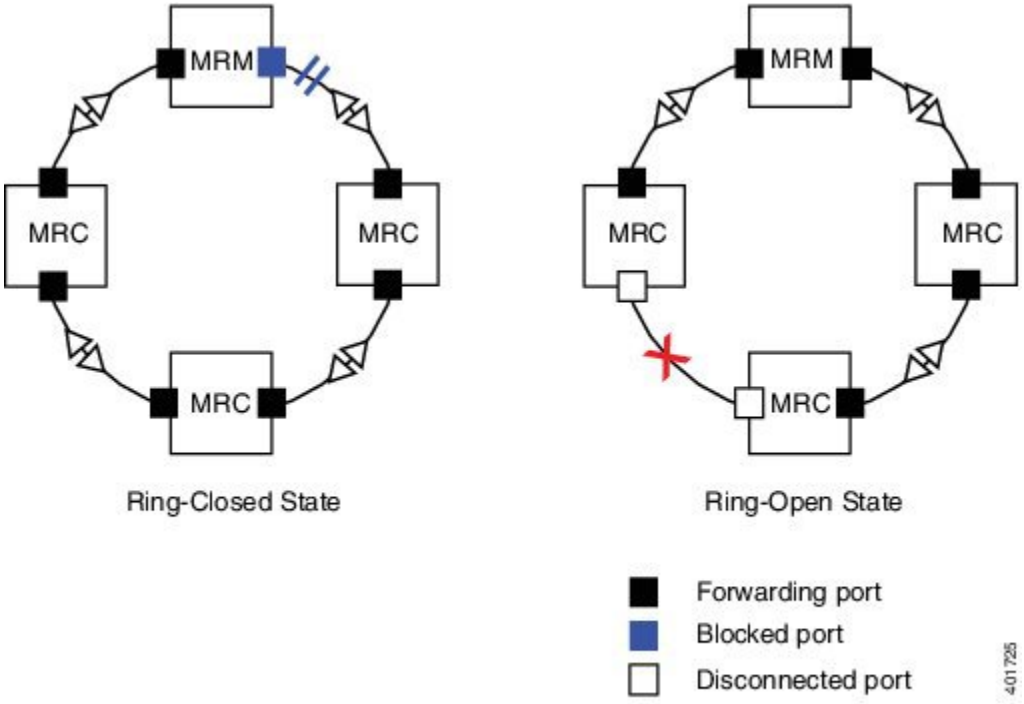
- Disabled: Ring ports drop all received frames.
- Blocked: Ring ports drop all received frames except MRP control frames and some standard frames, for example, LLDP.
- Forwarding: Ring ports forward all received frames.
- Not Connected: The link is physically down or disconnected. (This state differs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

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

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

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

Figure 1: MRP Ring States



If a network failure occurs:

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

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

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

MRP uses three types of control frames:

- To monitor the ring status, MRM regularly sends test frames on both ring ports.
- When MRM detects failure or recovery, it sends TopoChange frames on both ring ports.
- When MRC detects failure or recovery on a local port, it sends LinkChange subtype frames, Linkdown and Linkup, to the MRM.

Media Redundancy Automanager (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.

License Levels

For information about the licensing packages for features available on Cisco Catalyst IE3x00 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches and Cisco Catalyst IE3100 Rugged Series Switches, see Licensing on the Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches.

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 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

- 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 IE3100 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 IE3100 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.
- 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 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.
- 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.

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 switch boots at least one time, the GSD files for the switch are located in a directory called "ProfinetGSD". In this directory, there is a zip file containing all the GSDs for all the switch SKUs. 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.

Procedure

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.

Figure 2: PROFINET Device Discovery (DCP) Window Before Configuring MRP

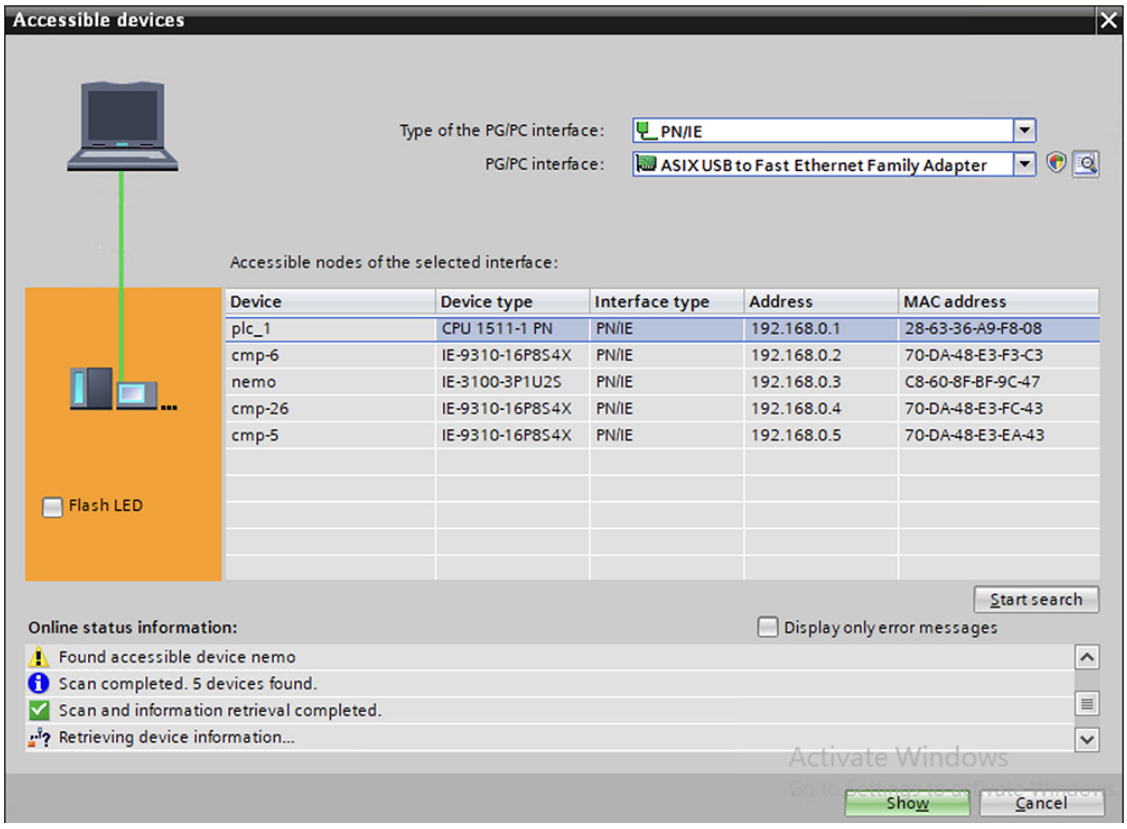


Figure 3: Define PROFINET MRP Manager and MRP domain

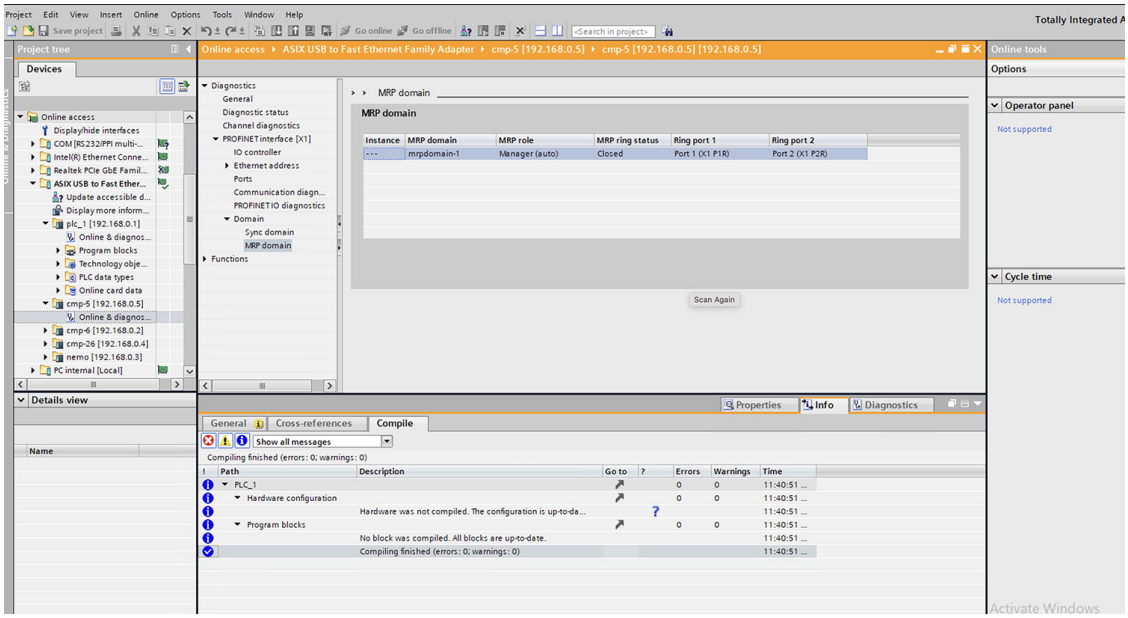


Figure 4: Define PROFINET MRP Client and MRP Domain

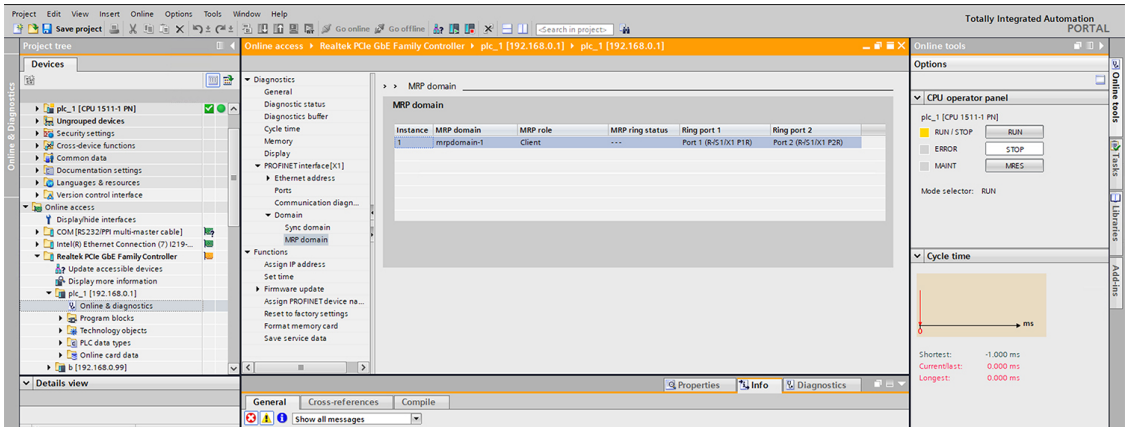


Figure 5: Define PROFINET MRP Interfaces

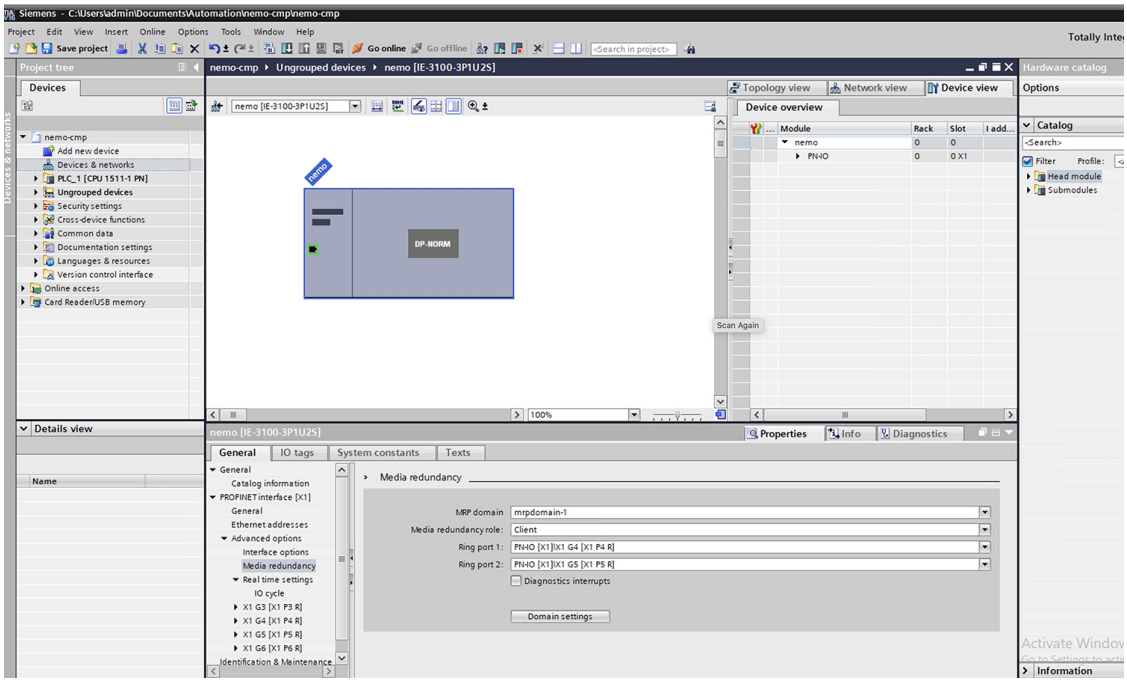
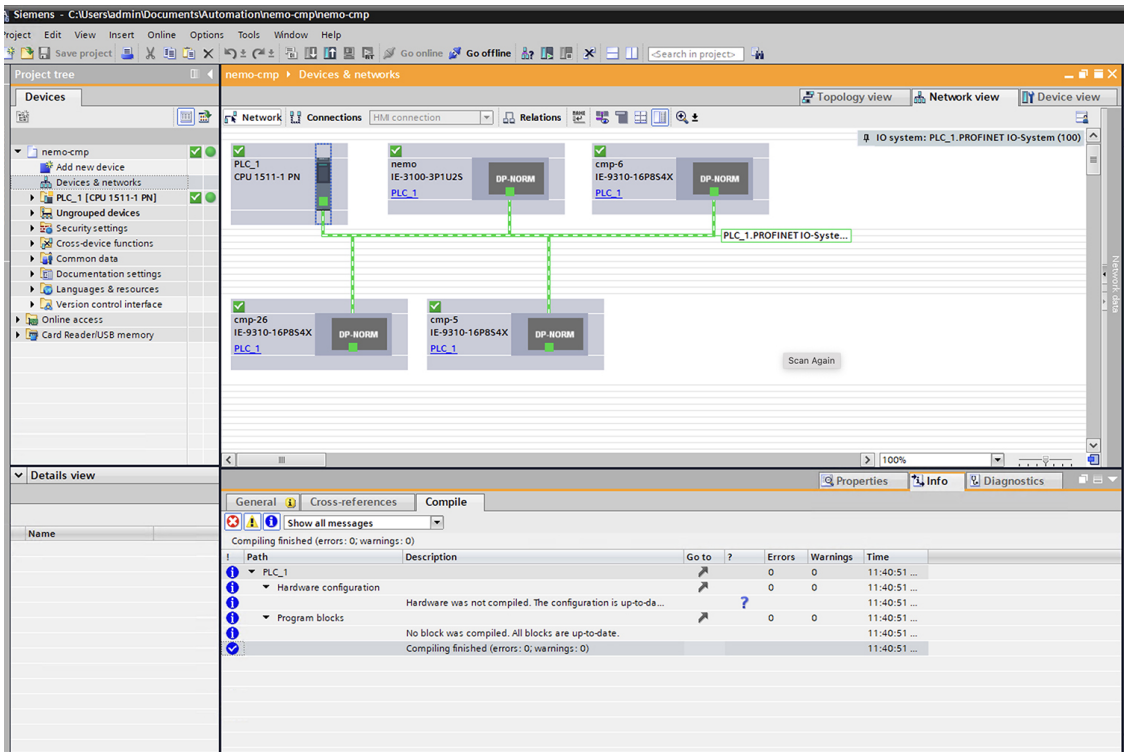


Figure 6: PROFINET MRP Network Configuration Diagram



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.
- 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.

Procedure

Step 1 Enter configuration mode:

configure terminal

no profinet mrp

Step 2 Enable MRP:

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:

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
```

```
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.

Configuring MRP Client

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

Procedure

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:

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
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.

Procedure

Step 1 Enter configuration mode:

configure terminal

Step 2 Enable PROFINET MRP:

profinet mrp

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.
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-support profinet	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.

Command	Description
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-support profinet	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
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
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:

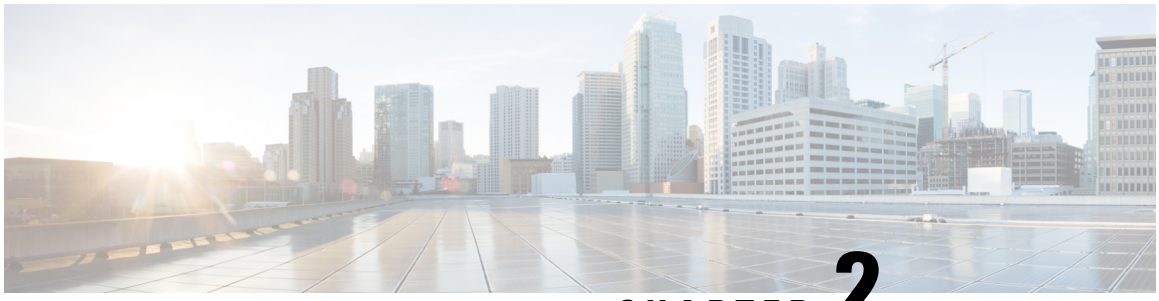
```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#mrp ring 1
Switch(config-mrp)#mode client
Switch(config-mrp-client)#end
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface gi1/3
Switch(config-if)#switchport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

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

Switch Platform	Feature	Initial Release
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



CHAPTER 2

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 Industrial Ethernet Series Switches with the Network Essentials license.

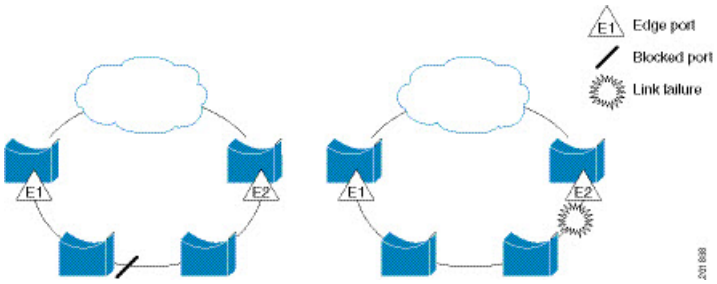
REP segment is a chain of ports connected to each other and configured with a same segment ID. Each segment consists of standard (non-edge) segment ports and two user-configured edge ports. A switch can have no more than two ports that belong to the same segment, and each segment port can have only one 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.

Note In a REP ring, when a REP node or a link to the REP node goes down, or when alternative or preferred ports do not detect the REP node on the REP ring, remove the primary edge and preferred ports, and reconfigure all the REP nodes as REP segments.

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.

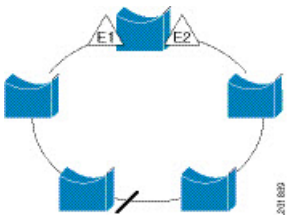
Figure 7: REP Open Segment



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 switch. With this configuration, you can create a redundant connection between any two switches in the segment.

Figure 8: REP Ring Segment



REP segments have the following characteristics:

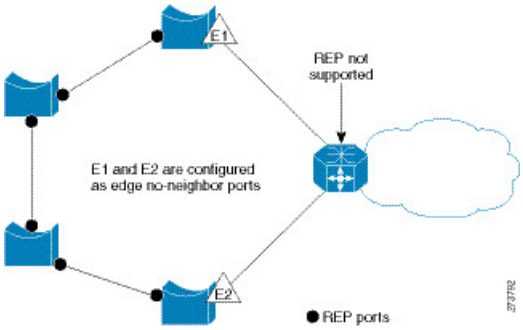
- If all ports in a segment are operational, one port (referred to as the ALT port) is in the blocked state for each VLAN. If VLAN load balancing is configured, two ALT ports in the segment control the blocked state of VLANs.
- If a port is not operational, and cause a link failure, all ports forward 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 9: Edge No-Neighbor Ports



REP has these limitations:

- You must configure each segment port; an incorrect configuration can cause forwarding loops in the networks.
- REP can manage only a single failed port within the segment; multiple port failures within the REP segment cause loss of network connectivity.
- You should configure REP only in networks with redundancy. Configuring REP in a network without redundancy causes loss of connectivity.

Link Integrity

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

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

A segment port does not become operational if:

- No neighbor has the same segment ID.
- More than one neighbor has the same segment ID.
- A neighbor does not acknowledge a local port as a peer.

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

Fast Convergence

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

VLAN Load Balancing

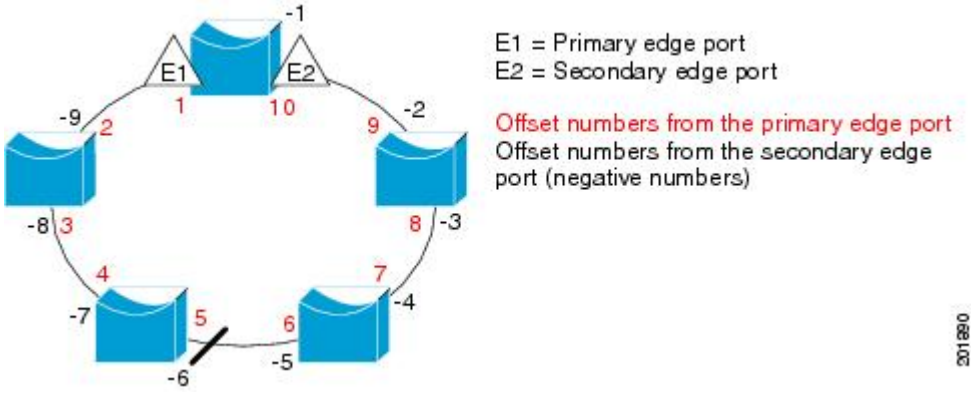
One edge port in the REP segment acts as the primary edge port; and another as the secondary edge port. It is the primary edge port that always participates in VLAN load balancing in the segment. REP VLAN balancing is achieved by blocking some VLANs at a configured alternate port and all the other VLANs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

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

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

The following figure shows neighbor offset numbers for a segment, where E1 is the primary edge port and E2 is the secondary edge port. The red numbers inside the ring are numbers offset from the primary edge port; the black numbers outside of the ring show the offset numbers from the secondary edge port. Note that you can identify all the ports (except the primary edge port) by either a positive offset number (downstream position from the primary edge port) or a negative offset number (downstream position from the secondary edge port). If E2 became the primary edge port, its offset number would then be 1 and E1 would be -1.

Figure 10: Neighbor Offset Numbers in a Segment



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

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

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

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

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

Reconfigure the primary edge port to reconfigure load balancing. When you change the load-balancing configuration, the primary edge port waits for the **rep preempt segment** command or for the configured preempt delay period after a port failure and recovery, before executing the new configuration. If you change an edge port to a regular segment port, the existing VLAN load-balancing status does not change. Configuring a new edge port might cause a new topology configuration.

Spanning Tree Interaction

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

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

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 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.

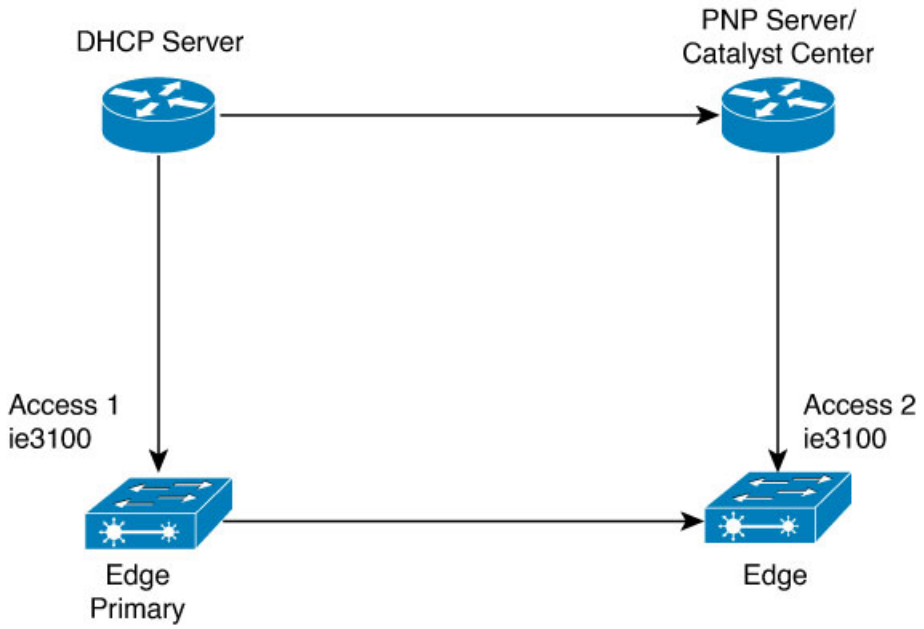
Note Starting IOS-XE release 17.17.1, 17.15.3, 17.12.5, 17.9.7, REP-Negotiated feature is deprecated. You can use REP-ZTP as an alternative.

REP and Day Zero

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

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

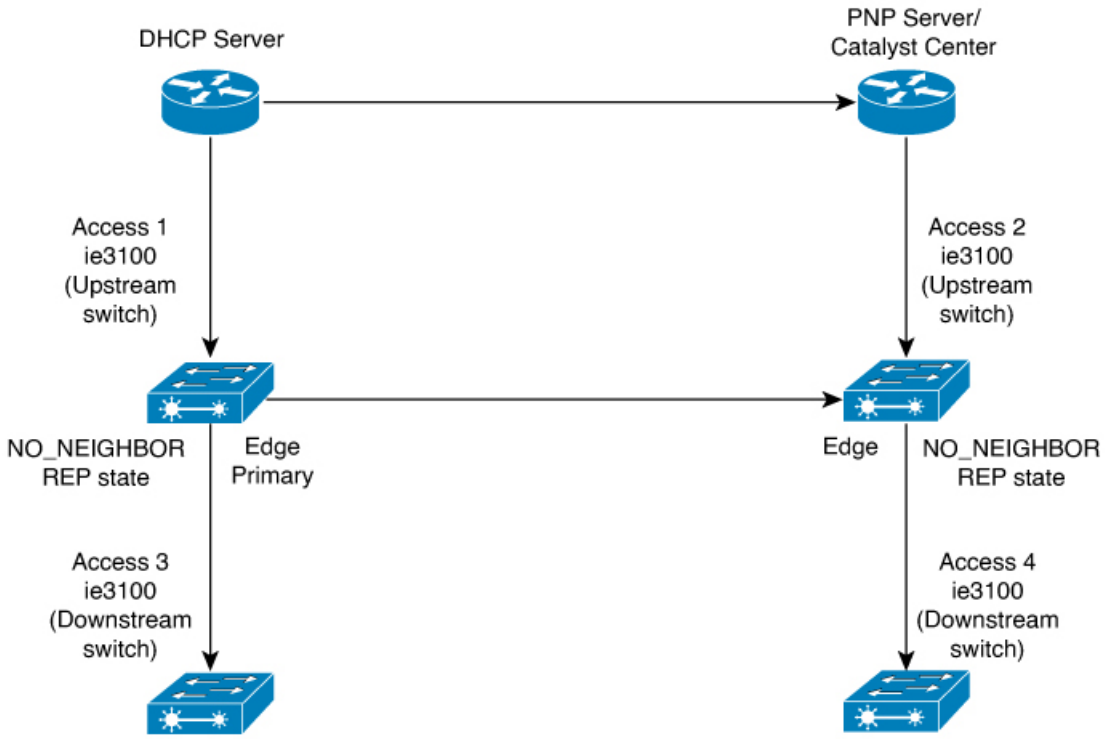
Figure 11: Adding Edge Nodes to the REP Ring



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

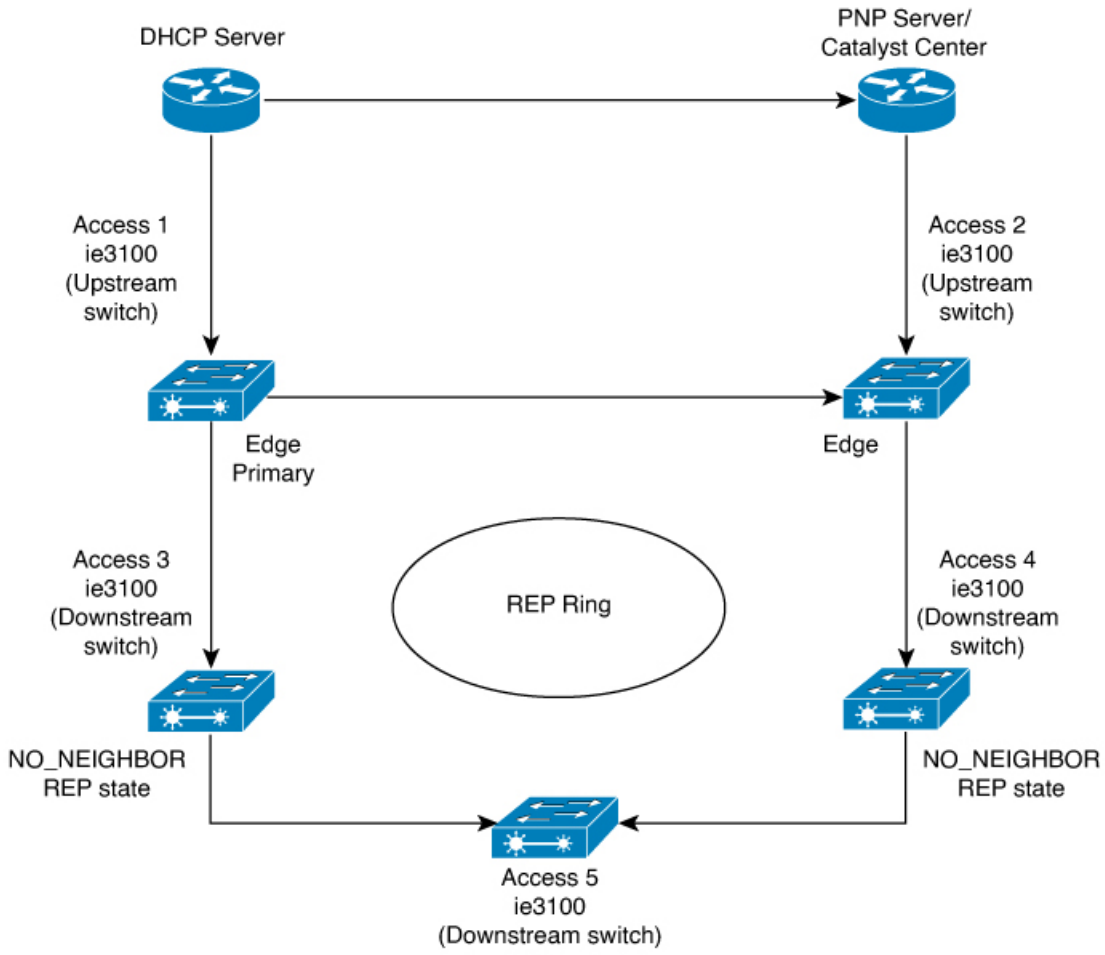
The first set of nodes to be provisioned are Access 1 and Access 2 in the diagram. These are the 2 edge nodes of the REP ring. Note that PnP has configured the downlink port as primary edge on Access 1 and secondary edge on Access 2.

Figure 12: Adding Downstream Nodes



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

Figure 13: 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).

Note From Cisco IOS XE Release 17.16.1, this feature is supported on the IE3100 on both physical interfaces and ether-channels.

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

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

The intent of this feature is to allow new switches to join a REP ring with no manual intervention. The interface on the upstream switch keeps the startup VLAN unblocked until the downstream switch has received its configuration and has configured its own interface for REP. If there's a failure in the PNP process, 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 44.

Note The upstream switch can be part of multiple REP rings and thereby connected to multiple downstream neighbors. 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.

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.

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.

- 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 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.
- For VLAN and VTP configuration, refer to the respective configuration guides.
- Before configuring the ring, refer to the relevant port configuration modes for access and trunk. Ensure that trunk configuration guidelines are followed.
- 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.
- 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 switch if you enable REP in a Telnet session that accesses the switch 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**. .
- 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.

- There can be a maximum of 5 REP segments per switch. If additional segments are needed, an expansion module can be connected to the base module.
- 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 Zero Touch Provisioning

- REP ZTP requires the PnP feature to be present on Cisco Catalyst IE3100switches.
- 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.
- REP ZTP on ether-channel is supported for IE3xxx and IE9300 from Cisco IOS XE 17.16.1 release onwards.
- 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.
- 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.

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

	Command or Action	Purpose
Step 3	**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. • (Optional) **preferred**—Indicates that the port is the preferred alternate port or the preferred port for VLAN load balancing.

	Command or Action	Purpose
		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

	Command or Action	Purpose
		number 1), you cannot enter an offset value of 1 to identify an alternate port. • **preferred**—Selects the regular segment port previously identified as the preferred alternate port for VLAN load balancing. • **vlan** *vlan-list*—Blocks one VLAN or a range of VLANs. • **vlan all**—Blocks all the VLANs. **Note** Enter this command only on the REP primary edge port.
Step 8	**rep preempt delay** *seconds* **Example:** `Device(config-if)# rep preempt delay 100`	(Optional) Configures a 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.

	Command or Action	Purpose
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 switch startup configuration file.

Setting Manual Preemption for VLAN Load Balancing

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

Procedure

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

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

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

Configuring SNMP Traps for REP

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

Procedure

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

Configuring REP ZTP

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

- Global level: Enabled
- Interface level: Disabled

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

Note When applying configuration from Catalyst Center or PNP server user must explicitly add this CLI configuration in the configuration template for the feature to be enabled.

Beginning with the Cisco IOS 17.16.1 release, you can configure the AVB as a Plug-n-Play feature using, a basic global enablement of AVB on all ports of the switch using the <no> avb <cr> configuration command.

Procedure

Step 1 Enter global configuration mode:

```
Switch# configure terminal
```

Step 2 Globally enable REP ZTP:

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

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

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

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

Step 4 Enable REP ZTP on the interface:

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

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

Step 5 Enable AVB on all ports of the switch:

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

Use the no form of the command to disable AVB: `Switch(config-if)#no avb`

Note
To make additional configurations for AVB use extended MSRP and gPTP commands. The Dynamic Reservation Entries prevent frames from being forwarded on ports where no MSRP reservation exists. These entries are similar to MAC address table entries and are created and managed by MSRP.

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.

Procedure

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 View Feature Status, on page 47 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.

Procedure

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 47 in this guide.

View Feature Status

You can use CLI commands to check the status of REP Segment-ID Autodiscovery on the segment.

Procedure

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
```

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:

```
switch#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
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.

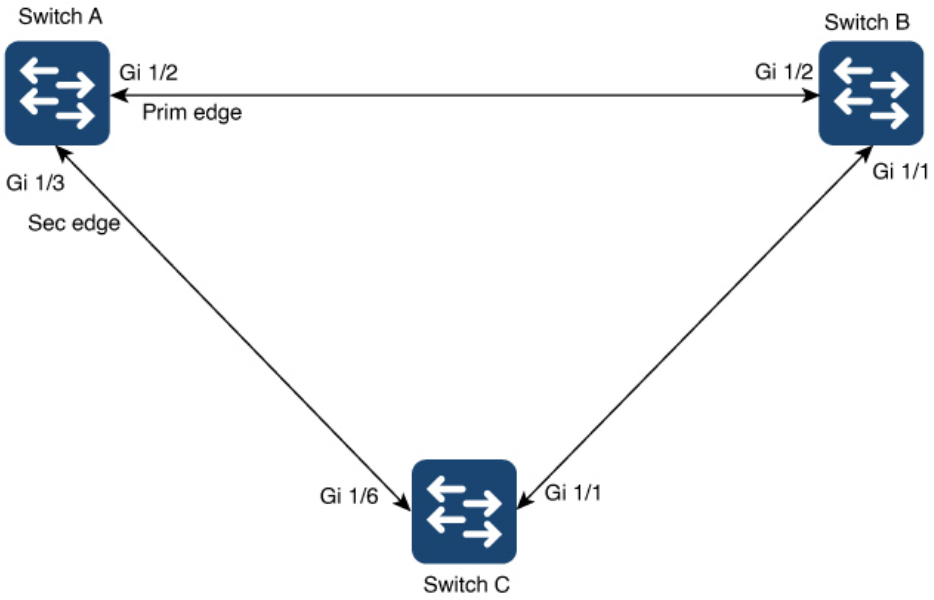
```
Device# show rep topology

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
```

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:

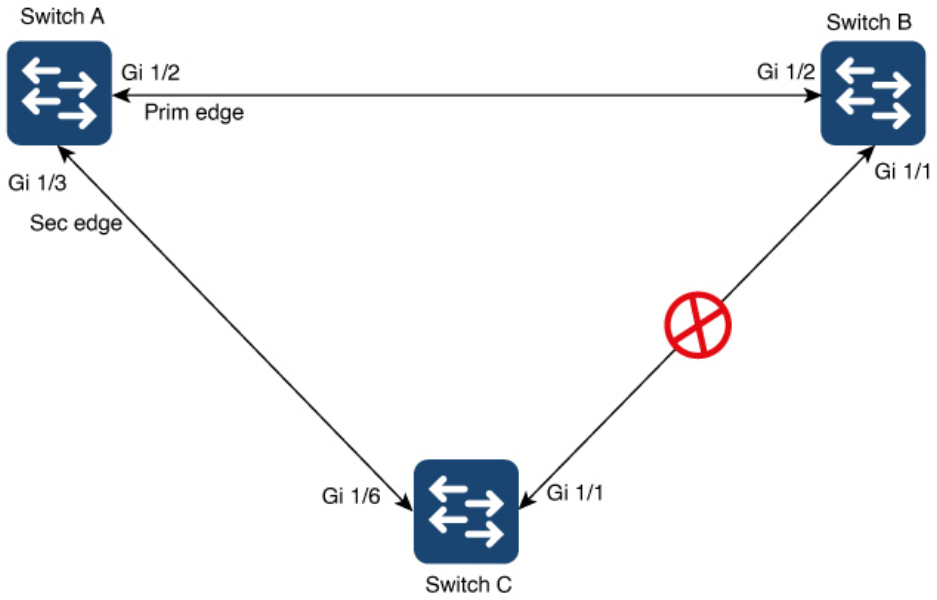
Figure 14: REP Closed Ring Topology




```
SWITCHA#sh rep topology
REP Segment 1
BridgeName                       PortName   Edge Role
-------------------------------- ---------- ---- ----
SWITCHA                          Gi1/2      Pri  Open
SWITCHB                          Gi1/2           Open
SWITCHB                          Gi1/1           Open
SWITCHC                          Gi1/1           Open
SWITCHC                          Gi1/6           Open
SWITCHA                          Gi1/3      Sec  Alt
```

Here is an example where the connection between SwitchB and SwitchC is down:

Figure 15: 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                          Gi1/2           Open
SWITCHB                          Gi1/1           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".

Procedure

Step 1 In privileged exec mode, enter:

show interfaces rep detail

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 Catalyst Center. The show command indicates the status as "Unblocked".

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

```
REP-6-ZTPPORTFWD: Interface GigabitEthernet1/2 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
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

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-Negotiated feature deprecation.	Starting IOS-XE release 17.17.1, 17.15.3, 17.12.5, 17.9.7, REP-Negotiated feature is deprecated. You can use REP-ZTP as an alternative.	Feature Deprecated.
REP Zero Touch Provisioning, supported on the IE3100 on both physical interfaces and ether-channels.	Cisco IOS XE 17.16.1	Initial support on Cisco Catalyst IE3100, IE3200, IE3300, IE3400, and IE9300.
REP Fast	Cisco IOS XE 16.11.1	Initial support on Cisco Catalyst IE3200, IE3300, and IE3400