

Resilient Ethernet Protocol

- Feature history for Resilient Ethernet Protocol, on page 1
- Resilient Ethernet Protocol, on page 2
- Resilient Ethernet Protocol Fast, on page 9
- REP Zero Touch Provisioning technologies, on page 11
- REP segment ID auto-discovery, on page 15
- REP segments, on page 17
- Preventive best practices, on page 27
- Monitoring REP configurations, on page 28
- PTP over REP , on page 32

Feature history for Resilient Ethernet Protocol

The table provides release and related information for the features documented in this guide.

Table 1: Feature History for Resilient Ethernet Protocol

Release	Feature	Feature Information
Cisco IOS XE 26.2.1	Enhanced scale limit	Starting from Cisco IOS XE release 26.2.1, REP Fast supports 26 open segments and 12 closed segments.
Cisco IOS XE 26.1.1	Enhanced scale limit	Starting with IOS-XE 26.1.1, a standalone Cisco Catalyst IE9300 Rugged Series Switch supports upto 26 open REP segments and 13 REP ring segments.
Cisco IOS XE 17.15.2	Resilient Ethernet Protocol	Starting with this release, the Cisco Catalyst IE9300 Rugged Series Switches supports up to 8 REP segments or 3 REP Fast segments. This is an increase from the previous limit of 4 REP segments or 3 REP Fast segments.

Release	Feature	Feature Information
Cisco IOS XE 17.14.x	Resilient Ethernet Protocol Zero Touch Provisioning	This feature was introduced in this release for Cisco Catalyst IE9300 Rugged Series Switches.
Cisco IOS XE Cupertino 17.9.x	Resilient Ethernet Protocol Fast	This feature was introduced in this release for Cisco Catalyst IE9300 Rugged Series Switches.

Resilient Ethernet Protocol

Resilient Ethernet Protocol (REP) is a Cisco proprietary protocol that provides an alternative to Spanning Tree Protocol (STP) to control network loops, handle link failures, and improve convergence time. REP controls a group of ports that are connected in a segment. It 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.

REP segments

A REP segment is a chain of ports that connect to each other and are configured with a segment ID. Each segment consists of standard (nonedge) segment ports and two user-configured edge ports. A switch can have no more than two ports that belong to the same segment. Each segment port can have only one external neighbor. A segment can pass through a shared medium. However, on any link, only two ports can belong to the same segment. REP operates only on trunk ports.

Characteristics of REP segments

REP segments have these characteristics.

- If all ports in a segment are operational, one port (called the ALT port) is blocked for each VLAN. If VLAN load balancing is configured, two ALT ports in the segment determine which VLANs are blocked.
- If a port is not operational, and causes a link failure, all ports forward traffic on all VLANs to ensure connectivity.
- In case of a link failure, alternate ports are unblocked as quickly as possible. When the failed link is restored, a logically blocked port per VLAN is selected with minimal disruption to the network.

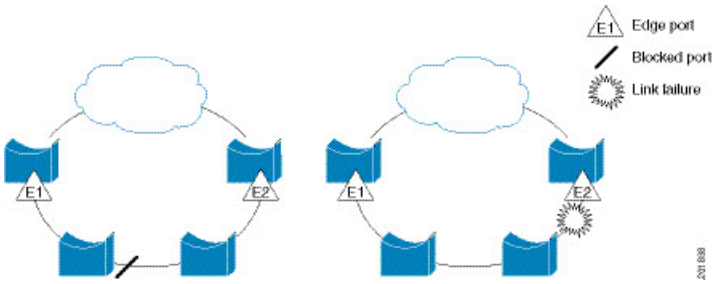
You can construct almost any type of network that is based on REP segments.

REP open segment

- Network Topology: The figure illustrates a network segment consisting of six ports distributed across four switches.
- Edge Port Configuration: Ports E1 and E2 are specifically configured as edge ports.
- Normal Operation: Under normal conditions (as shown in the left segment), one port is blocked to prevent network loops. This blocked port is marked with a diagonal line and is formally known as the **Alternate (ALT) port**.

- Network Failover: In the event of a network failure, the ALT port automatically transitions to a forwarding state to maintain connectivity and minimize service disruption.

Figure 1: REP open segment

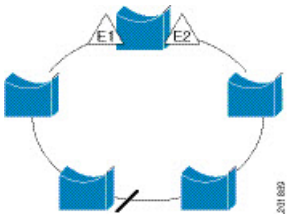


- Open Segment Status: The segment illustrated is an open segment. There is no direct connectivity between the two edge ports.
- Loop Prevention: Because the segment is open, it cannot cause a bridging loop, allowing you to safely connect the segment edges to any network.
- Connectivity and Redundancy: Hosts connected to switches within the segment have two potential paths to the rest of the network via the edge ports. Only one of these connections is active at any time to prevent loops.
- Failover Mechanism: If a failure occurs on any part of the REP segment, the protocol automatically unblocks the Alternate (ALT) port. This ensures that connectivity is maintained through the remaining available gateway.

REP ring segment

The segment shown in the figure is a closed segment, also called a ring segment. In this topology, both edge ports are located on the same switch. This configuration allows you to create a redundant connection between any two routers in the segment.

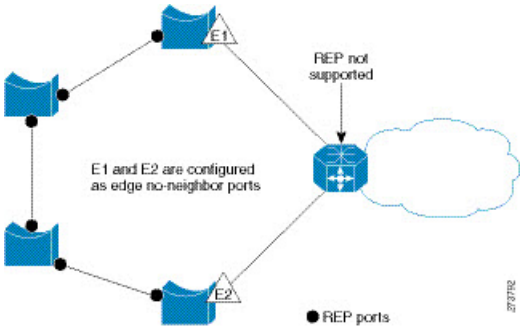
Figure 2: REP ring segment



Edge no-neighbor ports

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

Figure 3: 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.
- Only configure REP in networks with redundancy. If you configure REP in a network without redundancy, connectivity will be lost.

Link integrity detection

REP does not use an end-to-end polling function between edge ports to verify link integrity; instead, it implements local link failure detection. The REP Link Status Layer (LSL) detects its REP-aware neighbor and establishes connectivity within the segment. On an interface, all VLANs are blocked until the neighbor is detected. When REP identifies the neighbor, it selects the neighbor port to act as the alternate port and designates the ports that will forward traffic.

Port identification and initialization

Each port in a segment has a unique port ID. The port ID format is similar to the format used by the spanning tree algorithm: a port number (unique on the bridge) combined with a MAC address (unique in the network). When a segment port comes online, its LSL sends packets that include the segment ID and the port ID. The port becomes operational after successfully completing a three-way handshake with a neighbor in the same segment.

Conditions preventing port operation

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.

Neighbor adjacency and role assignment

Each port creates an adjacency with its immediate neighbor. After establishing neighbor adjacencies, the ports negotiate to select the blocked port for the segment, which functions as the alternate port. The remaining ports become unblocked.

REP packet transmission

By default, REP packets are sent to a bridge protocol data unit-class MAC address. Devices can also send packets to a Cisco multicast address, which is used only to transmit blocked port advertisement (BPA) messages during a segment failure. Devices that do not run REP drop these packets.

Fast convergence

- Protocol Efficiency: REP operates on a physical link basis rather than per-VLAN. This allows a single hello message to cover all VLANs, significantly reducing the protocol load.
- Configuration Requirements: To ensure proper operation, VLANs must be created consistently across all switches in a segment. Additionally, the same set of allowed VLANs must be configured on all REP trunk ports.
- Performance and Flooding: To minimize latency, REP can flood specific packets to a multicast address using the hardware flood layer (HFL). These messages are distributed throughout the entire network.
- External Handling: Switches located outside of the REP segment treat these HFL messages as standard data traffic.
- Flooding Control: You can manage and control the flooding of these messages by configuring an administrative VLAN for the entire domain or for a specific 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.

Specifying alternate port for VLAN load balancing

When you configure VLAN load balancing, you can specify the alternate port in one of the 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.

Configuring offset numbers

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.

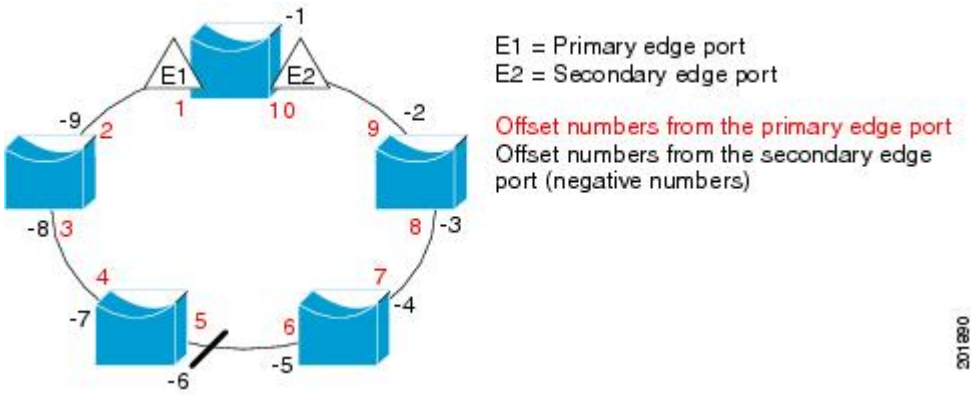
This figure shows neighbor offset numbers for a segment, where E1 is the primary edge port and E2 is the secondary edge port. The red numbers inside the ring are numbers offset from the primary edge port; the black numbers outside of the ring show the offset numbers from the secondary edge port.

You can identify all ports—excluding the primary edge port—using offset numbers:

- Positive offset: Indicates the port's position downstream from the primary edge port.
- Negative offset: Indicates the port's position downstream 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 4: Neighbor offset numbers in a segment



Configuring VLAN load-balancing triggers

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 the two ways:

- **Manual Trigger**: 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.
- **Preempt Delay Time**: 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.

VLAN load balancing execution

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.

Blocking all VLANs on a port

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.

Reconfiguring VLAN load balancing

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, you begin by configuring a single port in the ring as part of the segment. Next, configure 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. After configuring the segment in both directions up to the edge ports, configure the edge ports.

Resilient Ethernet Protocol (REP) Negotiated (Deprecated)



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 Spanning Tree Protocol (STP) are two different loop avoidance protocols. REP has certain advantages over STP in terms of convergence time. REP can be configured to run in a ring topology in such a way that it can provide the redundant path in case of a single link failure in the ring.

Cisco switches are STP enabled by default. If a switch that is STP enabled is inserted in an already running REP ring (for addition of a new node or replacement of existing node) the following conditions apply:

- The new switch will cause a break in the REP ring.
- The new switch will not be able to communicate over the ring until it is configured to be part of the REP ring.

The REP Negotiated feature tries to solve these issues by negotiating the REP status with the peers. The following table identifies when REP Negotiation events will trigger and the action to take. There are two events: both peers are negotiating, and neither peer is negotiating.

Note REP Negotiated works only on uplink ports.

SELF REP Negotiated	PEERS REP Negotiated	Event Triggered	Action
True	True	REPN	Configure REP
True	False	REPNN	Configure STP
False	X	REPNN	Remain in STP

This feature depends on 3 different protocols to get the required data and decide the correct configuration. The different protocols involved, and their purpose is given below:

- **STP**: By default, STP is enabled on all the ports on the Cisco Switch.
- **REP**: The customer network is configured to form a REP ring to provide better convergence time and redundancy.
- **Cisco Discovery Protocol (CDP)**: The feature depends on user defined TLVs sent through CDP messages to negotiate the correct (STP or REP) configuration for the interface.

REP ports

REP segments consist of Failed, Open, or Alternate ports:

- A port configured as a regular segment port starts as a failed port.
- After the neighbor adjacencies are determined, the port transitions to alternate port state, blocking all the VLANs on the interface. Blocked-port negotiations occur. When the segment settles, one blocked port remains in the alternate role, and all 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.

Converting a regular segment port to an edge port, or converting an edge port to a regular segment port, does not always result in a topology change. If you convert an edge port into a regular segment port, VLAN load balancing is not implemented unless it has been configured. For VLAN load balancing, you must configure two edge ports in the segment.

A segment port that is reconfigured as a spanning tree port restarts according to the spanning tree configuration. By default, this is a designated blocking port. If PortFast is configured or if STP is disabled, the port goes into the forwarding state.

Resilient Ethernet Protocol Fast

The Resilient Ethernet Protocol (REP) Fast feature allows faster link failure detection and convergence on the switch copper Gigabit Ethernet (GE) ports.

Note REP Fast is not supported on Trustsec.

REP design and link detection times

REP was originally designed for Fast Ethernet (FE 10/100) ports. On Fiber GE ports, link down detection time is also 10 ms. On GE copper interfaces, link drop detection and recovery times range from 750 ms to 350 ms. As a result, link loss and recovery are detected more quickly on GE fiber interfaces than on copper interfaces. Consequently, the convergence time for REP is much longer when using GE copper interfaces.

To improve link down detection time, the beacon mechanism triggers faster link failure detection (within 5–10 ms) when a REP interface is configured in REP Fast mode. The switch has two timers for each REP interface. The first timer is triggered every 3 ms to transmit the beacon frame to the neighbor node. After the frame is successfully transmitted and received, both timers are reset. If the packet is not received after transmission, the second timer is triggered to check reception within 10 ms. If the packet is not received when the timer expires, the switch sends a link down message.

Operation and compatibility

REP Fast operates on an individual link basis and does not affect the REP Protocol. Both ends of the link must support REP Fast for the feature to work. REP Fast can be used on any interface link pair configured for REP, but it was developed to address an issue on Gigabit copper links. It increases the speed of link failure detection on Gigabit copper interfaces.

Mixed REP and REP fast links

A REP Ring can have a mix of normal REP links and links with REP Fast. Interfaces with REP Fast transmit 3000 packets a second as part normal operation. Enabling REP Fast does not affect REP ring size, because it operates only on the interfaces configured for it. Because REP Fast has to generate Beacon frames, only six interfaces on a single REP node can be configured for REP Fast at a time.

Convergence and compatibility requirements

If the neighbor acknowledges and is configured for REP Fast mode, convergence occurs within 50 ms. If a neighbor switch does not support the REP Fast feature, normal REP mode must be used for link up/down detection. In this case, you must disable fast mode on both ends of the link.

For information about configuring REP Fast, see Configure REP Fast in this guide.

Configure REP Fast

Follow these steps to configure REP Fast:

Before you begin

Enable REP on the switch and configure the REP topology as described in Configuring REP.

Procedure

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

Step 2 Use the **interface** *interface-id* command to specify the interface and enter interface configuration mode.

Step 3 Use the **REP fastmode** command to enable REP Fast.

Step 4 Use the **end** command to return to privileged exec mode.

Example

```
gabitEthernet 1/0/1
switch-RJ(config-if)#rep seg
switch-RJ(config-if)#rep segment ?
<1-1024> Between 1 and 1024

switch-RJ(config-if)#rep segment 10
switch-RJ(config-if)#rep fastmode
switch(config)#int <interface number>
switch(config-if)#
switch(config-if)#rep ?
  fastmode       REP fastmode
switch (config-if)#rep fastmode ?
  <cr>  <cr>

switch#sh run int <interface number>
Building configuration...

Current configuration : 89 bytes
!
interface <interface number>
 switchport mode trunk
 rep segment <segment id>
 rep fastmode
end
switch#

switch#sh run int <interface number>
Building configuration...

Current configuration : 89 bytes
!
interface <interface number>
 switchport mode trunk
 rep segment <segment id>
 rep fastmode
end
```

REP Zero Touch Provisioning technologies

REP Zero Touch Provisioning (ZTP) is a feature that enables automated provisioning of REP rings in a network, eliminating the need for manual configuration during device deployment.

- Automates the configuration of REP rings using zero-touch technologies.
- Introduces a new TLV extension into REP LSL packets.
- Reduces manual intervention required for Day 0 REP ring provisioning.

How REP ZTP works

ZTP technologies automate bringing devices such as routers and switches into a functional state with little or no manual configuration. The Cisco Network Plug and Play (PnP) and autoinstall Day 0 solutions offer a unified, secure approach to help enterprise and industrial network customers simplify device rollouts and provisioning updates.

However, PnP does not support REP because of REP's design. Prior to the REP ZTP feature, REP ring provisioning for Day 0 required manual intervention. The REP ZTP feature introduces a new TLV extension into the REP LSL packets to support configuring REP rings with zero-touch technologies.

Day 0 processes

Zero Touch Provisioning (ZTP) and Cisco PnP process enable a switch with no startup configuration to automatically obtain its configuration from a DHCP and PnP server.

- Switches with no startup configuration trigger the Cisco PnP agent to initiate DHCP discovery.
- The DHCP server provides IP configuration and the address or hostname of the PnP server using option 43.
- The PnP server downloads the required Day 0 configuration to the switch to complete provisioning.

ZTP deployment workflow

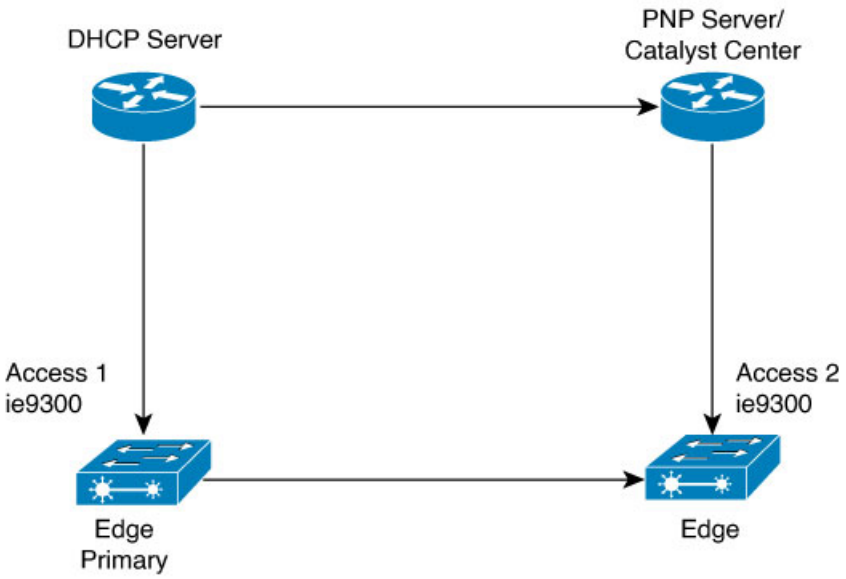
- Initiation: A switch without a startup configuration triggers the Cisco PnP agent to begin a DHCP discovery process.
- Identification: Upon receiving a DHCP DISCOVER message with Option 60 ("cisco pnp"), the DHCP server responds with the PnP server's address via Option 43.
- Connection: The switch's PnP agent extracts the PnP server information from the DHCP response to establish a direct connection.
- Provisioning: The PnP server completes the process by deploying the required Day 0 configuration to the switch.



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

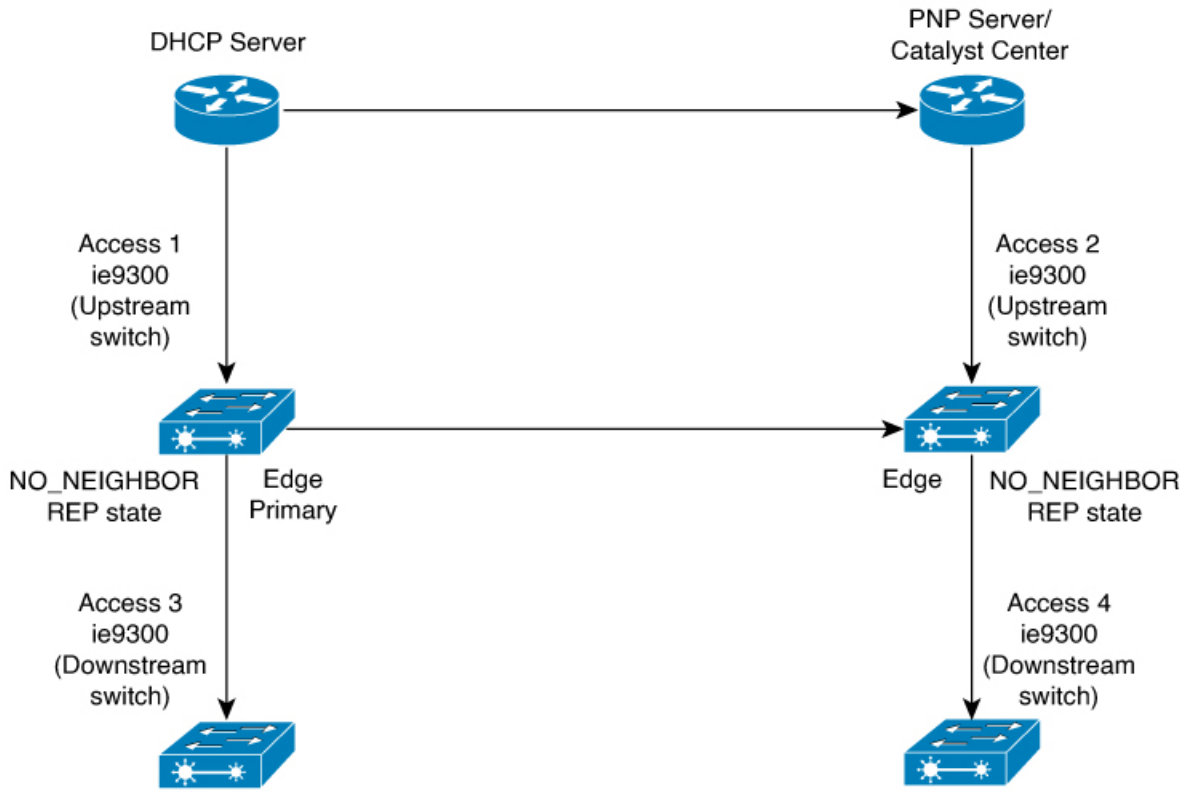
The example diagrams illustrate REP ring provisioning on Day 0, prior to the introduction of REP ZTP.

Figure 5: Adding edge nodes to the REP ring



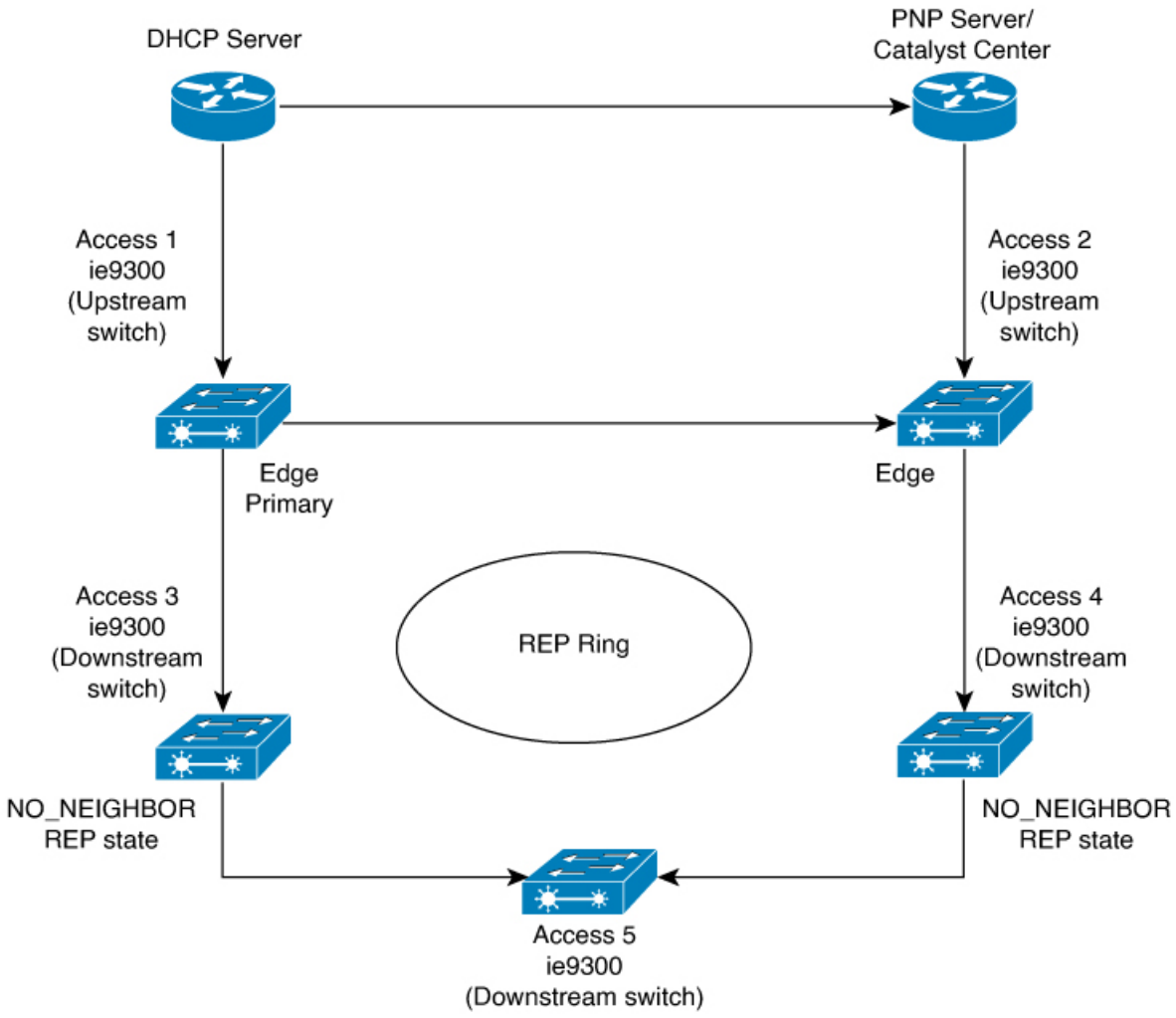
The first set of nodes to be provisioned are Access 1 and Access 2 in the diagram. These are the 2 edge nodes of the REP ring. Note that PnP has configured the downlink port as primary edge on Access 1 and secondary edge on Access 2.

Figure 6: Adding downstream nodes



- When Access 3 or Access 4 is powered on, the REP edge primary port initiates negotiation and detects that the neighbor is not REP-enabled.
- Since switches require PnP provisioning via DHCP to join the REP ring, they must first contact the DHCP server. However, an upstream REP port enters the NO_NEIGHBOR state when it fails to discover a REP peer.
- In this NO_NEIGHBOR state, the port blocks all VLAN traffic, preventing the new switch's DHCP discovery messages from reaching the server.
- This blockage stalls the PnP provisioning process and persists for every subsequent switch added to the ring until the initial provisioning issue is resolved.

Figure 7: NO_NEIGHBOR REP state



REP ZTP features

REP ZTP mechanisms are Zero Touch Provisioning protocols for REP rings that

- enables upstream switches to temporarily unblock the PNP startup VLAN for downstream switches during provisioning,
- allows new switches to join a REP ring automatically, and
- requires both upstream and downstream switches to support REP ZTP.

How REP ZTP works and operational considerations

When a 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).

To enable REP ZTP provisioning, follow these steps involving REP LSL packets, TLV signaling, VLAN unblocking, and interface configuration.

- The upstream switch transmits REP LSL packets to the downstream.
- The downstream switch (with REP ZTP enhancement) sends REP LSL packets with a new TLV, signaling an attempt to provision.
- Upon recognizing this TLV, the upstream switch unblocks the PNP startup VLAN for that interface only.
- The downstream switch completes PNP provisioning over the unblocked VLAN.
- Once configuration is complete (including REP enablement), or on failure, the upstream interface returns the PNP VLAN to blocked state.
- To activate this behavior, the upstream switch must have the interface explicitly configured with the **rep ztp-enable** command.
- The PNP startup VLAN is unblocked only on interfaces connected to the downstream joining switch, even if the upstream switch is in multiple REP rings.
- Downstream switches transmit the REP LSL with the new TLV by default when no startup configuration exists.

Note For more on configuration, see Configure REP ZTP, on page 25.

REP segment ID auto-discovery

A REP segment ID auto-discovery feature is a network feature that

- automatically configures and retains segment IDs in REP segments,
- allows switches to learn and store segment ID information through dedicated CLI commands, and
- supports both standard REP and REP Fast protocols starting with Cisco IOS XE 26.1.x or later.

REP segment ID auto-discovery reference information

REP segment ID auto-discovery reduces manual configuration errors and supports deployments with multiple REP rings by automating segment ID assignment and retention. This feature simplifies the process of adding switches to existing REP segments or creating new ones without manual intervention.

REP segment ID auto-discovery deployment

REP Segment-ID auto-discovery allows for simplified configuration when adding a switch to a REP segment or creating a new REP segment, reducing manual configuration in both scenarios.

- Auto-discovery can be enabled when adding a switch to an existing REP segment or when building a new segment.
- Manual configuration steps are reduced by using REP segment-ID auto-discovery.

- Deployment order and configuration steps vary depending on whether you are adding a switch, building a new segment, or building a segment with uplinks.

Add new switch to a REP segment

- When you add a switch to an existing REP segment, use the **rep autodisc** command on the switches connected to the upstream and downstream devices to enable auto-discovery.
- After connecting the new switch, the upstream and downstream switches send Cisco Discovery Protocol (CDP) packets with REP segment ID information to the new switch interfaces.
- Use the **rep segment auto** command on the new switch interfaces. This action allows the interfaces to learn the segment ID.

Build 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 apply to both closed and open REP segments. Begin by bringing up the next node in the REP ring. Then, add a new node between the two switches to enable auto-discovery.

Build 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 auto-discovery on the connected uplink. Port pairing support duplicates the REP configuration on the paired uplink port.
- After connecting each device to the uplink, the process repeats to bring the REP segment in a daisy chain manner. Each new REP node joins the ring automatically by learning the REP segment ID from its connected node. In an REP open ring, the last device on the segment acts as an edge device with static REP configuration.

REP segment ID auto-discovery limitations

- The only supported port-pairing is uplinks Gi1/0/25 - Gi1/0/26, and Gi1/0/27 - Gi1/0/28. The same pairing applies to Ten Gigabit Ethernet (Te) ports.
- If you configure a REP segment on a downlink port, the switch receives the segment ID from the upstream switch and connects the partner downlink port to the same segment. However, the switch does not pass the segment ID to its partner port. As a result, you must configure the partner port of the downlink pair manually.
- This feature does not support the insertion of an edge node into an existing segment. You must configure static or manual REP segment IDs on both the primary and secondary edge devices.
- When inserting a new switch between two existing segment switches, connect the interface of the new switch to the corresponding interfaces on the existing switches that transmit the same segment ID. If you

connect the interfaces incorrectly, the segment will fail. You must meet this requirement when removing a node between two others.

For example, if Gi1/0/1 of switch1 and Gi1/0/2 of switch2 are part of an existing segment, and you insert switch3 between them, ensure that the interfaces connect to Gi1/0/1 of switch1 and Gi1/0/2 of switch2. This approach includes switch3 in the same segment.

- If you configure REP automatically on an interface using the **rep segment auto** command, and later remove the REP configuration with the **no rep segment** or overwrite it with the **rep segment** command, you cannot configure REP automatically again by using the **rep segment auto** command. To restore automatic configuration, shut down the interface, bring it up, and enter the **rep segment** auto command again.
- REP segment ID auto-discovery depends on the CDP protocol. It does not support EtherChannel links.

REP segments

A segment is a collection of ports that are connected to one another in a chain and configured with a segment ID.

- Each segment is defined by a unique segment ID.
- Ports within a segment are connected in a chain topology.
- Segments require the configuration of primary and secondary edge ports.

Configuring REP segments and edge ports

To configure REP segments, you must set the REP administrative VLAN (or use the default VLAN 1) and add the desired ports to the segment in interface configuration mode.

Follow these configuration requirements and guidelines:

- Configure the REP administrative VLAN or use VLAN 1 by default.
- Add ports to the segment using interface configuration mode.
- Configure two edge ports in a segment. Assign one port as the primary edge port and the other as the secondary edge port, which is the default setting.
- Only one primary edge port should exist in a segment.
- If two ports are configured as primary edge ports, REP selects one to serve as the segment's primary edge port.
- Optionally, configure the location for segment topology change notices (STCNs) and VLAN load balancing.

Default REP configurations

A default REP configuration is a network protocol setting that

- disables REP on all interfaces by default, with interfaces acting as regular segment ports unless specifically configured as edge ports,

- sets the initial conditions for VLANs and administrative VLANs (all VLANs blocked, administrative VLAN is VLAN 1, STCNs disabled when REP is enabled), and
- determines the behavior of advanced features, such as VLAN load balancing (manual preemption as default; delay timer disabled) and REP fast or REP ZTP (REP fast disabled; REP ZTP enabled globally and disabled at interface level).
- If VLAN load balancing is not configured, after manual preemption, the system blocks all VLANs on the primary edge port.
- REP fast is disabled by default.
- REP ZTP is enabled by default at the global level, but disabled at the interface level.

Guidelines and limitations for REP configuration

Follow these guidelines when configuring REP:

- The IE9300 switch supports up to 8 REP segments or 3 REP fast segments starting from IOS-XE release 17.15.2. Earlier releases supported a maximum of 4 REP segments or 3 REP fast segments.
- We recommend starting with one port and then configuring contiguous ports to minimize both the number of segments and blocked ports.
- If more than two ports in a segment fail and no external neighbors are configured, a single port transitions to a forwarding state, maintaining connectivity for the data path during configuration.

  In the **show interfaces rep** command output, the Port Role for this port displays as 'Fail Logical Open', and the Port Role for the other failed port displays as **Fail No Ext Neighbor**. After external neighbors are configured for the failed ports, they transition through alternate port states; they eventually move to an open state or remain as the alternate port, as determined by 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.
- Use caution when configuring REP over an SSH or Telnet connection. REP blocks all VLANs until another REP interface sends an unblock message. If you enable REP on the same interface used for the SSH or Telnet session, you may lose connectivity to the switch.
- You cannot run REP and STP on the same segment or interface.
- If you connect an STP network to a REP segment, ensure the connection is at the segment edge. Connecting STP to a non-edge location may cause a bridging loop, as STP does not operate on REP segments and all STP BPDUs are dropped at REP interfaces.
- If REP is enabled on two ports of a switch, both ports must be configured as either regular segment ports or edge ports. REP ports must meet these requirements:
  - Only two ports on a switch can be part of 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 both be edge ports, both regular segment ports, or one regular port and one edge no-neighbor port. An edge port and a regular segment port 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 the other as a regular segment port (a misconfiguration), the edge port will be treated as a regular segment port.

- REP interfaces initially come up in a blocked state and remain blocked until it is safe to unblock. Monitor interface status to prevent unexpected 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 the duration for which a REP interface remains active without receiving a hello from a neighbor. You can use the **rep lsl-age-timer** interface configuration command to set the time range from 120 ms to 10,000 ms. The LSL hello timer is then set to the age-timer value divided by three. In normal operation, three LSL hellos are sent before the age timer on the peer switch expires and checks for hello messages. Only use **rep lsl-age-timer** for non-REP fast copper Gigabit interfaces. All other interfaces do not benefit from **rep lsl-age-timer**.
    - EtherChannel port-channel interfaces do not support LSL age-timer values less than 1000 ms. If you attempt to configure a value below 1000 ms on a port channel, an error message will be displayed, and the command will be rejected.
    - **lsl-age-timer** interface-level command is intended to be used when normal link down detection will be too slow for convergence time.

      FastEthernet and fiber connections do not require the **lsl-age-timer**. Gigabit copper interfaces can use REP fast instead.

- REP ports cannot be configured as any of these port types:
    - Switched Port Analyzer (SPAN) destination port
    - Tunnel port
    - Access port
- REP is supported on EtherChannels, but not on individual ports within an EtherChannel.
- REP ring size is unlimited; however, rings with more than 20 nodes may experience slow convergence.

Guidelines for REP fast configuration

Follow these guidelines when configuring REP fast:

- You must configure REP fast on both ends of the link in order for the feature to work.
- A REP segment can contain a mix of Gigabit fiber and Gigabit copper. The 50 ms requirement for convergence from a single failure can be achieved if Gigabit copper interfaces have REP fast.
- REP fast can be deployed within a REP segment where not all interfaces support REP fast; however, 50ms convergence may not be guaranteed in such cases.
- Be aware of these limitations:
    - A maximum of three REP segments can have REP fast enabled at the same time.
    - Beginning with release 26.1.1, MACsec can interoperate with both REP and REP fast. Before this release, MACsec interoperated only with REP fast.

- REP fast is not supported in a stacked environment.
- REP fast over EtherChannel is not supported.

Guidelines for REP ZTP configuration

Follow these guidelines when configuring REP ZTP:

- Ensure that the PnP feature is present on Cisco Catalyst IE9300 Rugged series switches to enable REP ZTP functionality.
- Understand that REP behavior during the NO_NEIGHBOR state is modified beginning in Cisco IOS XE 17.14.1 and later. This change allows a DHCP request message to reach a DHCP server and unblock PnP provisioning of a new switch, with no impact to the REP state machine after PnP completion.
- Apply the changes in REP behavior during the NO_NEIGHBOR state only to REP ZTP in Cisco IOS XE 17.14.1 and later. If the PnP feature is not present, normal REP functionality operates as expected.
- The REP ZTP feature can coexist with the REP bpduleak/negotiated feature on fiber uplink ports.
- Do not use the REP ZTP feature on EtherChannel interfaces for day 0 on an upstream switch, as EtherChannel is not present on the downstream interface by default. REP ZTP operates only on physical interfaces.
- REP ZTP is supported on both copper (downlink) and fiber (uplink) interfaces.
- REP ZTP interoperates only with other IE switching products running IOS XE that claim REP ZTP support.

Configure the REP administrative VLAN

When a link fails or a VLAN is blocked during load balancing, REP floods packets to a regular multicast address at the HFL. Flooding occurs throughout the entire network. It does not occur only within the REP segment. You can control message flooding by configuring an administrative VLAN.

Before you begin

Use 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, complete these steps.

Procedure

Step 1 Use the **enable** command to enter privileged EXEC mode.

Enter your password if prompted.

Step 2 Use the **configure terminal** command to enter global configuration mode.

Step 3 Use the **rep admin vlan** *vlan-id* command to configure the administrative VLAN.

Example:

```
Switch(config)# rep admin vlan 2
```

Specifies the administrative VLAN. The range is from 2 to 4094.

Step 4 (Optional) Use the **no rep admin vlan** command to reset the admin VLAN to the default (1).

Step 5 Use the **end** command to exit global configuration mode.

Step 6 (Optional) Use the **show interface** *[interface-id]* **rep detail** command to verify REP configuration on the interface.

Example:

```
Switch# show interface gigabitethernet1/0/1 rep detail
```

Step 7 (Optional) Use the **copy running-config startup config** command to save your entries in the switch startup configuration file.

Configure a REP interface

To configure REP, enable REP on each segment interface and identify the segment ID.

Perform this task to enable and configure REP on IW916x APs using the CLI.

Before you begin

Ensure the following prerequisites are met:

- You need interface IDs, segment IDs, and VLAN lists.

Procedure

Step 1 Use the **interface** *interface-id* command to select the interface to configure.

Example:

```
Switch(config)#interface gigabitethernet1/0/1
```

Specifies the interface, and enters interface configuration mode. The interface can be a physical Layer 2 interface or a port channel (logical interface).

Step 2 Use the **switchport mode trunk** command to configure the interface as a Layer 2 trunk port.

Step 3 Use the **rep segment** *segment-id* [**edge** [**no-neighbor** | **primary**] | **preferred**] command to enable REP on the interface and identify segment parameters.

The segment ID range is from 1 to 1024.

Example:

```
Switch(config-if)# rep segment 10
```

Note
You must configure both a primary edge port and a secondary edge port on 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.

  ```
  Switch(config-if)# rep segment 10 edge
  ```

- (Optional) **no-neighbor** : Configures a port with no external REP neighbors as an edge port. The port inherits all the properties of an edge port, and you can configure the properties the same way you do for an edge port.

  ```
  Switch(config-if)# rep segment 10 edge no-neighbor
  ```

- (Optional) **primary** : Configures the port as the primary edge port, the port on which you can configure VLAN load balancing.

  ```
  Switch(config-if)# rep segment 10 edge primary
  ```

  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.

  ```
  Switch(config-if)# rep segment 10 preferred
  ```

  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 4 (Optional) Use the **rep stcn** [**interface** *interface-id* |**segment** *id-list* | **stp**] command to configure STCNs as needed.

These keywords are available:

- **interface** *interface-id*: Designates a physical interface or port channel to receive STCNs.

  ```
  Switch(config-if)# rep stcn interface GigabitEthernet1/0/48
  ```

- **segment** *id-list* : Identifies one or more segments to receive STCNs. The range is from 1 to 1024.

  ```
  Switch(config-if)# rep stcn segment 10, 20
  ```

- **stp** : Sends STCNs to STP networks.

  ```
  Switch(config-if)# rep stcn stp
  ```

Note
Multiple 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 5 (Optional) Use the **rep block port** [**id** *port-id* | *neighbor-offset* | **preferred**] **vlan** [*vlan-list* | **all**] command to configure VLAN load balancing on the primary edge port.

Example:

```
Switch(config-if)# rep block port id 0009001818D68700 vlan 1-100
```

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.

These keywords are available to configure VLAN load balancing:

- **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
  When you enter the **rep block port** command at the primary edge port (offset number 1), you cannot enter an offset value of 1 to identify an alternate port.

- **preferred** : Selects the regular segment port previously identified as the preferred alternate port for VLAN load balancing.
- **vlan** *vlan-list*: Blocks one VLAN or a range of VLANs.
- **vlan all**: Blocks all the VLANs.

Note
Enter this command only on the REP primary edge port.

Step 6 (Optional) Use the **rep preempt delay** *seconds* command to set a pre-empt delay for VLAN load balancing.

Example:

```
Switch(config-if)#rep preempt delay 100
```

- Use this command if you want VLAN load balancing to be automatically triggered after a link failure and recovery.
- The time delay range is between 15 to 300 seconds. The default is manual pre-emption with no time delay.

Note
Enter this command only on the REP primary edge port.

Step 7 (Optional) Use the **rep lsl-age-timer** *value* command to configure the REP interface aging timer.

Example:

```
Switch(config-if)#rep lsl-age-timer 2000
```

Configures a time (in milliseconds) for which the REP interface remains up without receiving a hello from a neighbor.

The range is from 120 to 10,000 ms in 40-ms increments. The default is 5000 ms (5 seconds).

Note
- EtherChannel port channel interfaces do not support LSL age-timer values that are less than 1000 ms.
- Ensure that both the ports on the link have the same LSL age configured in order to avoid link flaps.

Step 8 Use the **end** command to exit global configuration mode and returns to privileged EXEC mode.

Step 9 (Optional) Use the **show interface** [*interface-id*] **rep** [**detail**] command to displays the REP interface configuration.

Example:

```
Switch# show interface gigabitethernet1/0/1 rep detail
```

Manually trigger VLAN load balancing on a segment

To manually trigger VLAN load balancing on a specified segment using the CLI, especially when no preemption delay is configured.

If you do not configure a preemption time delay using the **rep preempt delay** *seconds* interface configuration command on the primary edge port, VLAN load balancing must be triggered manually on the segment by default. Complete all other segment configurations before manually triggering VLAN load balancing. A confirmation message appears when you use the **rep preempt delay segment** *segment-id* command, as preemption can cause network disruption.

Before you begin

- Ensure you have completed all other segment configuration steps.
- Make sure you are at the device CLI with appropriate privileges.

Procedure

Step 1 Use the **enable** command to enable the privileged EXEC mode.

Enter your password if prompted.

Step 2 Use the **rep preempt segment** *segment-id* command to manually trigger VLAN load balancing on the segment.

Example:

```
Switch# rep preempt segment 100
The command will cause a momentary traffic disruption.
Do you still want to continue? [confirm]
```

You need to confirm the command before it is executed.

Step 3 (Optional) Use the **show rep topology segment** *segment-id* command to view the current REP topology information for the specified segment.

Example:

```
Switch# show rep topology segment 100
```

Step 4 Use the **end** command to exit configuration mode and return to privileged EXEC mode.

Configure 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

Step 1 Use the **enable** command to enable privileged EXEC mode.

Enter your password if prompted.

Step 2 Use the **configure terminal** command to enter global configuration mode to make changes to device settings.

Step 3 Use the **snmp mib rep trap-rate** *value* command to enable the switch to send REP traps and sets the number of traps sent per second.

Example:

```
Switch(config)# snmp mib rep trap-rate 500
```

Enter the number of traps sent per second. The range is 0 to 1000. The default value is 0, which means no limit is imposed and a trap is sent at every occurrence.

Step 4 Use the **end** command to return to privileged EXEC mode.

Step 5 (Optional) Use the **show running-config** command to view the running configuration, which can be used to verify the REP trap configuration.

Step 6 (Optional) Use the **copy running-config startup-config** command to save your entries in the switch startup configuration file.

Configure REP ZTP

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

- Global level: Enabled
- Interface level: Disabled

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



Note When applying configuration from DNAC or a PNP server, the user must explicitly add this CLI command to the configuration template to enable the feature.

Procedure

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

Step 2 Use the **rep ztp** command to globally enable the REP ZTP.

Note
Use the **no rep ztp** command to disable REP ZTP.

Step 3 Use the **interface** *interface-name* command to enter interface configuration mode on the upstream device interface that is connected to the downstream device.

Example:

```
Switch(config)# interface GigabitEthernet1/0/1
```

Step 4 Use the **rep ztp-enable** command to enable REP ZTP on the interface.

Note
Use the **no rep ztp-enable** command to disable REP ZTP on the interface.

The following example shows the minimum configuration required to enable the REP ZTP feature on the upstream device interface that is connected to a downstream device.

```
Switch#show running-config interface gigabitEthernet 1/0/1
Building configuration...
Current configuration : 93 bytes
!
interface GigabitEthernet1/0/1
switchport mode trunk
rep segment 100
rep ztp-enable
end
```

Configure REP segment ID auto-discovery

Perform this task during new REP ring deployments, during ring expansions, or when you want to minimize manual configuration steps. Completing this process simplifies ring deployments and speeds up the work.

Before you begin

- Verify that your switch model and software version support REP segment ID auto-discovery. To confirm support, enter **rep ?** in global configuration mode and verify that **rep-auto-discovery** appears in the help output.
- Identify the devices to configure as edge nodes. These nodes require static configuration.
- Ensure that CDP is enabled on all devices.

Perform these steps to configure REP segment ID auto-discovery:

Procedure

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

Step 2 Use the **rep autodisc** command to configure REP auto discovery.

Note
Use the **no rep autodisc** command to disable the REP segment ID.

Step 3 Use the **interface** *interfacename interface-id* command to enter the interface configuration mode.

Example:

```
Switch(config)# interface GigabitEthernet1/0/1
```

Step 4 Use the **rep segment auto** command to enable auto-discovery on an interface that participates in the REP ring.

Note
Use the **no rep segment** command to disable auto-discovery.

Step 5 Use the **rep segment** *segment-id* **edge** command to configure static REP on edge nodes with static REP segment ID.

Example:

```
Switch(config-if)# rep segment 100 edge
```

Step 6 (Optional) Use the **show interfaces rep detail** command to check the status of REP segment ID auto-discovery on the segment.

Example:

This example shows that the REP segment ID auto-discovery is globally enabled on a device.

```
Switch# show interfaces rep detail
REP Segment Id Auto Discovery Status: Enabled
```

This example shows that the REP segment ID auto-discovery is globally disabled on a device.

```
Switch# show interfaces rep detail
REP Segment Id Auto Discovery Status: Disabled
```

This example shows that the REP segment ID on the interface is configured automatically.

```
Switch# show interfaces rep detail
REP Segment Id Type: Auto
```

This example shows that the REP segment ID on the interface is configured manually.

```
Switch# show interfaces rep detail
REP Segment Id Type: Manual
```

Preventive best practices

Control-plane load governance

Ensure overall control-plane load is kept within safe limits to avoid interference with critical protocols such as REP, BFD, and PTP.

- Configure monitoring tools and SNMP polling intervals conservatively to prevent excessive CPU utilization.
- Account for concurrent CPU-intensive features, such as high-frequency SNMP polling, PTP traffic bursts, and BFD sessions, especially during topology changes or reconvergence events.
- Operate devices on stable and recommended software releases to benefit from validated fixes, performance improvements, and resiliency enhancements.

PTP and topology change stabilization

- Reduce transient CPU spikes that timing and topology adjustments can cause.
- Allow sufficient stabilization time for PTP after topology changes to reduce short-term CPU utilization increases.
- Avoid overlapping PTP adjustments with REP reconvergence or other CPU-intensive events.

REP design and operational planning

Design and operate REP with simplicity and predictability to minimize control-plane impact.

- Design REP rings only when operationally necessary. Avoid excessive, overlapping, or unnecessary rings that can increase reconvergence time and CPU load.
- Review and tune REP timing parameters, such as **rep preempt delay**, to align with resiliency goals and operational requirements.
- Plan configuration changes, maintenance windows, and REP topology modifications carefully to avoid multiple simultaneous control-plane events.

CPU monitoring and diagnostics

Continuously monitor system health to detect and mitigate CPU stress early.

- Monitor CPU utilization trends, particularly during REP convergence, power events, and maintenance activities.
- Periodically review system logs and resource utilization for recurring or sustained CPUHOG events linked to REP or other control-plane processes.
- Enable and retain sufficient logging and diagnostic data to support effective troubleshooting during abnormal conditions.

Recommended operational checks

Use these commands to monitor system state and collect diagnostic information.

- **show processes cpu sorted**
- **show platform resource**
- **show rep topology**
- **show logging**
- **show tech-support**

Monitoring REP configurations

This topic provides examples of REP monitoring command output. The examples show configuration and status details for uplink and downlink ports as well as segment topology information.

This section provides example outputs for the **show interface** [*interface-id*] **rep** [**detail**] command. The output shows REP configuration and status on both uplink and downlink ports.

The **show interface** [*interface-id*] **rep** [**detail**] command output demonstrates the REP configuration and status on a uplink port.

```
 Device# show interfaces GigabitEthernet1/0/4 rep detail
GigabitEthernet1/0/4 REP enabled
Segment-id: 3 (Primary Edge)
PortID: 03010015FA66FF80
Preferred flag: No
```

```
Operational Link Status: TWO_WAY
Current Key: 02040015FA66FF804050
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
REP-ZTP Status: Disabled
Preempt Delay Timer: disabled
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 999, tx: 652
HFL PDU rx: 0, tx: 0
BPA TLV rx: 500, tx: 4
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 6, tx: 5
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 135, tx: 136
```

The **show interface** [*interface-id*] **rep** [**detail**] command output demonstrates the REP configuration and status on a downlink port.

```
Device# show interface GigabitEthernet1/0/5 rep detail
GigabitEthernet1/0/5   REP enabled
Segment-id: 1 (Segment)
PortID: 019B380E4D9ACAC0
Preferred flag: No
Operational Link Status: NO_NEIGHBOR
Current Key: 019B380E4D9ACAC0696B
Port Role: Fail No Ext Neighbor
Blocked VLAN: 1-4094
Admin-vlan: 1
REP-ZTP Status: Disabled
Preempt Delay Timer: 100 sec
LSL Ageout Timer: 2000 ms
LSL Ageout Retries: 5
Configured Load-balancing Block Port: 09E9380E4D9ACAC0
Configured Load-balancing Block VLAN: 1-100
STCN Propagate to: segment 25
LSL PDU rx: 292, tx: 340
HFL PDU rx: 0, tx: 0
BPA TLV rx: 0, tx: 0
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 0, tx: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 0, tx: 0
```

This section provides an example output for the **show rep topology** [**segment** *segment-id*] [**archive**] [**detail**] command. The output displays REP topology information for all segments.

```
Device# show rep topology
REP Segment 1
BridgeName       PortName     Edge Role
---------------- ----------   ---- ----
10.64.106.63     Gi1/0/4      Pri  Open
10.64.106.228    Gi1/0/4           Open
10.64.106.228    Gi1/0/3           Open
10.64.106.67     Gi1/0/3           Open
10.64.106.67     Gi1/0/4           Alt
10.64.106.63     Gi1/0/4      Sec  Open
```

```
REP Segment 3
BridgeName       PortName     Edge Role
---------------- ----------   ---- ----
10.64.106.63     Gi1/011     Pri  Open
SVT_3400_2       Gi1/0/3           Open
SVT_3400_2       Gi1/0/4           Open
10.64.106.68     Gi1/0/2           Open
10.64.106.68     Gi1/0/1           Open
10.64.106.63     Gi1/0/2      Sec  Alt
```

Check the REP ZTP status

Use the **show** command to identify the state of REP ZTP on an interface. In this example, REP ZTP is disabled on interface GigabitEthernet 1/0/1 and enabled on interface GigabitEthernet 1/0/2.

Procedure

Step 1 Use the **show interfaces rep detail** command in the privileged exec mode.

Example:

```
GigabitEthernet1/0/1 REP enabled
Segment-id: 100 (Segment)
PortID: 00016C13D5AC4320
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 00026C13D5AC43209DAB
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1

REP-ZTP Status: Disabled
REP Segment Id Auto Discovery Status: Enabled
REP Segment Id Type: Manual
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
LSL Ageout Retries: 5
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 382, tx: 297
HFL PDU rx: 0, tx: 0
BPA TLV rx: 1, tx: 19
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 95, tx: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 95, tx: 95
GigabitEthernet1/0/2 REP enabled
Segment-id: 100 (Segment)
PortID: 00026C13D5AC4320
Preferred flag: No
Operational Link Status: NO_NEIGHBOR
Current Key: 00026C13D5AC43209DAB
Port Role: Fail No Ext Neighbor
Blocked VLAN: 1-4094
Admin-vlan: 1
REP-ZTP Status: Enabled
```

```
REP-ZTP PnP Status: Unknown
REP-ZTP PnP Vlan: 1
REP-ZTP Port Status: Blocked

REP Segment Id Auto Discovery Status: Enabled
REP Segment Id Type: Manual
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
LSL Ageout Retries: 5
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 11, tx: 11
HFL PDU rx: 0, tx: 0
BPA TLV rx: 0, tx: 0
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 0, tx: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 0, tx: 0
```

Step 2 Use the **show interfaces rep detail** command to monitor the status of **REP ZTP**.

When the downstream device is booted up, it sends notification to the connected upstream switch interface, which unblocks the **pnp_startup_vlan** so the device can obtain a DHCP IP address and establish communication with the PNP server or DNAC. The show command indicates the status as Unblocked.

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

```
REP-6-ZTPPORTFWD: Interface GigabitEthernet1/0/2 moved to forwarding on ZTP notification
```

```
REP-6-ZTPPORTBLK: Interface GigabitEthernet1/0/2 moved to blocking on ZTP notification
```

Example:

```
Switch#show interfaces rep detail
GigabitEthernet1/0/1 REP enabled
Segment-id: 100 (Segment)
PortID: 00016C13D5AC4320
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 00026C13D5AC43209DAB
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
REP-ZTP Status: Disabled
REP Segment Id Auto Discovery Status: Enabled
REP Segment Id Type: Manual
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
LSL Ageout Retries: 5
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 430, tx: 358
HFL PDU rx: 0, tx: 0
BPA TLV rx: 1, tx: 67
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 107, tx: 0
```

```
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 107, tx: 108

GigabitEthernet1/0/2 REP enabled
Segment-id: 100 (Segment)
PortID: 00026C13D5AC4320
Preferred flag: No
Operational Link Status: NO_NEIGHBOR
Current Key: 00026C13D5AC43209DAB
Port Role: Fail No Ext Neighbor
Blocked VLAN: 1-4094
Admin-vlan: 1
REP-ZTP Status: Enabled
REP-ZTP PnP Status: In-Progress
REP-ZTP PnP Vlan: 69
REP-ZTP Port Status: Unblocked
REP Segment Id Auto Discovery Status: Enabled
REP Segment Id Type: Manual
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
LSL Ageout Retries: 5
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 32, tx: 40
HFL PDU rx: 0, tx: 0
BPA TLV rx: 0, tx: 0
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 0, tx: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 0, tx: 0
```

Step 3 Use the **show platform hardware l2 stp** command to check the interface state of the PnP startup VLAN.

Example:

```
Switch#show platform hardware l2 stp asic-num 0 vlan-id 69 □[PnP Vlan]
------------------------STP TABLE START------------------------
---------------------------------------------------------------
VlanId:1 StpId:0 MemberPort:3 StpState:FORWARDING
VlanId:1 StpId:0 MemberPort:7 StpState:FORWARDING
VlanId:1 StpId:0 MemberPort:25 StpState:FORWARDING
---------------------------------------------------------------
------------------------STP TABLE END-------------------------
```

Step 4 (Optional) Use these 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.

PTP over REP

PTP over REP is a time synchronization solution that:

- combines Precision Time Protocol (PTP) with Resilient Ethernet Protocol (REP),

- provides accurate and predictable time synchronization in ring and linear Layer 2 topologies, and
- maintains timing continuity during link or node failures in industrial networks.

PTP over REP is essential for environments that require accurate timing for applications such as motion control, protection relays, and distributed control systems. It also ensures that network resiliency does not cause timing reconvergence events that disrupt these applications.

REP ensures rapid topology recovery, while PTP maintains synchronization accuracy across the restored topology.

Use cases

Common PTP over REP use cases include:

- An industrial ring network that uses REP for fast failover and PTP to synchronize controllers and field devices.
- A linear REP topology that connects network nodes in industrial environments where precise time alignment is required for monitoring and protection applications.

Guidelines for PTP over REP

- Each Boundary Clock (BC) introduces additional delay at every hop.
- Transparent Clock (TC) deployments minimize per-hop delay contribution. TCs are limited to a single VLAN.
- PTP over REP supports both standard REP and REP Fast. When using REP Fast, configure REP Fast on all ports in the ring. Do not mix standard REP and REP Fast within the same ring.

PTP clock types profiles and their accuracy

Table 2: PTP clock types, profiles, and their accuracy

Platforms	PTP clock type	PTP profile	PTP accuracy	Number of REP rings
Cisco Catalyst IE9300 Rugged Series Switch	• Boundary Clock • Grandmaster Boundary Clock • Transparent Clock	Default (IEEE 1588 v2), Power 2011/2017	Boundary Clock (BC): ~200 ns per hop Transparent Clock (TC): ~50 ns per hop	Up to 26 open REP segments

Platforms	PTP clock type	PTP profile	PTP accuracy	Number of REP rings
Cisco IE3500 Rugged Series Switch	• Boundary Clock • Grandmaster Boundary Clock • Transparent Clock	Default Profile (IEEE 1588 v2), Power Profile 2011/2017	Boundary Clock (BC): ~200 ns per hop Transparent Clock (TC): < 200 ns per hop	Up to 26 open REP segments or 3 REP Fast segments

Note

- End-to-end accuracy depends on the cumulative delay introduced by the number of BCs and TCs in the network path.
- The stated PTP accuracy values do not apply when GLC-T copper SFP transceivers are used in the timing path because these transceivers can reduce PTP timing accuracy.

Table 3: PTP over REP capabilities

Category	Support
PTP clocks	• Boundary Clock • Grandmaster Clock • Transparent Clock
PTP profiles	• Default (IEEE 1588 v2) • Power Profile 2011/2017 (platform-dependent)
Media	• Copper ports • SFP-based fiber ports
REP topology	• Ring topologies • Linear topologies • Up to 26 REP rings
VLAN behavior	• Boundary Clocks support multiple VLANs. • Transparent Clocks support a single VLAN.

Configure PTP over REP

You can configure PTP over REP using either of the following profiles:

- Configure PTP over REP using default profile
- Configure PTP over REP using power profile

Configure REP

Configures REP on switch interfaces to enable ring topology and PTP packet transport by setting the administrative VLAN and segment membership for ring ports.

Procedure

Step 1 Create and activate VLAN:

a) Use the **configure terminal** command to enter global configuration mode.

Example:

```
Switch# configure terminal
```

b) Use the **vlan** *vlan-id* command to create VLAN configuration on the switch, which serves as both the REP administrative VLAN and the PTP transport VLAN.

Example:

```
Switch(config)# vlan 100
```

c) (Optional) Use the **no shutdown** command in VLAN configuration mode to ensure that VLAN is administratively enabled.

Example:

```
Switch(config-vlan)# no shutdown
```

Note
This command applies to the Layer 2 VLAN and not an SVI. It helps clear an existing `lshut` state in a brownfield network.

The **lshut** status means that the VLAN is locally shut down.

d) Use the **exit** command to return to global configuration mode.

Example:

```
Switch(config-vlan)# exit
```

Step 2 Configure REP on interface:

a) Use the **interface** *interface-id* command to configure the interface.

Example:

```
Switch(config)# interface GigabitEthernet1/3
```

b) Use the **switchport mode trunk** command on the interface to set the first ring-facing port to trunk mode, allowing VLAN-tagged traffic including PTP packets to pass through.

Example:

```
Switch(config-if)# switchport mode trunk
```

c) Use the **switchport trunk allowed vlan** *vlan-id* command to explicitly permit VLAN on the trunk, ensuring PTP messages are not blocked by VLAN filtering.

Example:

```
Switch(config-if)# switchport trunk allowed vlan 100
```

d) Use the **rep segment** *segment-id* command to add interface as a non-edge member, enabling it to participate in the resilient ring topology and carry PTP packets.

Example:

```
Switch(config-if)# rep segment 10
```

e) Use the **no shutdown** command to enable the interface.

Example:

```
Switch(config-if)# rep segment 10
```

f) Use the **exit** command to return to global configuration mode.

Example:

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

g) Use the **rep admin vlan** *vlan-id* command to configure VLAN as the REP administrative VLAN to ensure REP control messages and PTP packets share the same VLAN and are not filtered.

Example:

```
Switch(config)# rep admin vlan 100
```

Repeat step 2 to configure REP on the second interface.

Step 3 (Optional) Use the **show rep topology** command to verify that the switch ports appear in REP segmen topology with `Open` state before proceeding with PTP configuration.

Example:

```
Switch# show rep topology
REP Segment 10

BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
RB1              Gi4/0/7    Pri  Open
Switch           Gi1/3           Open
Switch           Gi1/4           Open
RB2              Gi2/0/7         Open
RB2              Gi2/0/8         Alt
LANB-1           Gi1/4           Open
LANB-1           Gi1/3           Open
RB1              Gi4/0/8    Sec  Open
```

Configure PTP over REP using power profile

Configure PTP over REP using the power profile to enable precise time synchronization across industrial ring topologies.

Before you begin

Ensure REP is configured.

Procedure

Step 1 Clear the existing PTP configuration.

a) Use the **configure terminal** command to enter global configuration mode.

Example:

```
Switch# configure terminal
```

b) Use the **no ptp profile** command to remove any existing PTP profile configuration before applying a new one.

Example:

```
Switch(config)# no ptp profile
```

c) Use the **no ptp mode** command to remove any existing PTP mode configuration on the switch.

Example:

```
Switch(config)# no ptp mode
```

d) Use the **no ptp domain** command to remove any existing PTP domain configuration on the switch.

Example:

```
Switch(config)# no ptp domain
```

Step 2 Configure REP on an interface.

a) Use the **interface** *interface-id* command to configure the interface.

Example:

```
Switch(config)# interface GigabitEthernet1/3
```

b) Use the **rep segment** *segment-id* command to add the interface as a non-edge member, enabling it to participate in the resilient ring topology and carry PTP packets.

Example:

```
Switch(config-if)# rep segment 10
```

c) Use the **exit** command to return to global configuration mode.

Example:

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

Repeat step 2 to configure REP on the second interface.

Step 3 Configure PTP power profile, mode, and domain.

a) Use the **ptp profile power** command to configure the power profile on the switch.

Example:

```
Switch(config)# ptp profile power
```

b) Use the **ptp mode p2ptransparent** command to configure the switch as a peer-to-peer Transparent Clock (TC) under the power profile.

Example:

```
Switch(config)# ptp mode p2ptransparent
```

c) Use the **ptp domain** *domain-number* command to assign the switch to PTP domain, ensuring it participates in the correct PTP synchronization domain.

Example:

```
Switch(config)# ptp domain 100
```

Step 4 Use the **interface** *interface-id* command to configure the first REP ring-facing interface and enter interface configuration mode.

Example:

```
Switch(config)# interface GigabitEthernet1/3
```

Step 5 Use the **ptp vlan** *vlan-id* command on the interface to bind PTP operation to VLAN on the first REP ring-facing interface.

Example:

```
Switch(config-if)# ptp vlan 100
```

Step 6 Use the **exit** command to return to global configuration mode.

Example:

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

Repeat steps 4 to 6 to configure PTP VLAN on the other ring-facing interface.

Step 7 Verify the REP configuration.

Example:

```
Switch# show rep topology
REP Segment 10

BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
RB1              Gi4/0/7    Pri  Open
Switch           Gi1/3           Open
Switch           Gi1/4           Open
RB2              Gi2/0/7         Open
RB2              Gi2/0/8         Alt
LANB-1           Gi1/4           Open
LANB-1           Gi1/3           Open
RB1              Gi4/0/8    Sec  Open
```

Configure PTP over REP using default profile

Configure PTP over REP using the default profile to enable precise time synchronization across industrial ring topologies.

Before you begin

Ensure REP is configured.

Procedure

Step 1 Use these commands to clear the existing PTP configuration:

a) Use the **configure terminal** command to enter global configuration mode.

Example:

```
Switch# configure terminal
```

b) Use the **no ptp profile** command to remove any existing PTP profile configuration before applying a new one.

Example:

```
Switch(config)# no ptp profile
```

c) Use the **no ptp mode** command to remove any existing PTP mode configuration on the switch.

Example:

```
Switch(config)# no ptp mode
```

d) Use the **no ptp domain** command to remove any existing PTP domain configuration on the switch.

Example:

```
Switch(config)# no ptp domain
```

Step 2 Configure REP on an interface:

a) Use the **interface** *interface-id* command to select the interface and enter interface configuration mode.

Example:

```
Switch(config)# interface GigabitEthernet1/3
```

b) Use the **rep segment** *segment-id* command to add the interface as a nonedge member, enabling it to participate in the resilient ring topology and carry PTP packets.

Example:

```
Switch(config-if)# rep segment 10
```

c) Use the **exit** command to return to global configuration mode.

Example:

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

Repeat step 2 to configure REP on the second interface.

Step 3 Configure PTP mode and domain:

a) Use the **ptp mode e2etransparent** command to configure the switch as an end-to-end Transparent Clock (TC).

Example:

```
Switch(config)# ptp mode e2etransparent
```

b) Use the **ptp domain** *domain-number* command to assign the switch to PTP domain, ensuring it participates in the correct PTP synchronization domain.

Example:

```
Switch(config)# ptp domain 100
```

c) Use the **end** command to return to privileged EXEC mode.

Example:

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

Step 4 (Optional) Use the **show rep topology** command to verify the REP configuration.

Example:

```
Switch# show rep topology
REP Segment 10
BridgeName   PortName   Edge   Role
------------ ---------- ----   ----
RB1          Gi4/0/7    Pri    Open
Switch       Gi1/3              Open
Switch       Gi1/4              Open
RB2          Gi2/0/7            Open
RB2          Gi2/0/8            Alt
LANB-1       Gi1/4              Open
LANB-1       Gi1/3              Open
RB1          Gi4/0/8    Sec    Open
```