LAN Switching Configuration Guide, Cisco IOS XE Gibraltar 16.12.x (Cisco NCS 520 Series)

First Published: 2019-07-31

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.

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.

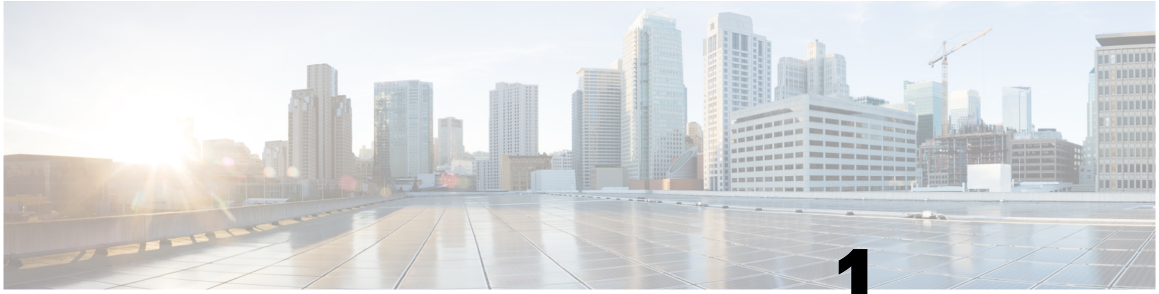
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY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

CONTENTS



CHAPTER 1

Configuring Resilient Ethernet Protocol

The Resilient Ethernet Protocol (REP) is a Cisco proprietary protocol that provides an alternative to the Spanning Tree Protocol (STP). REP provides a way to control network loops, handle link failures, and improve convergence time. It 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 complex networks and supports VLAN load balancing.

Note The convergence value is improved from Cisco IOS XE 3.17 release.

Restrictions for Resilient Ethernet Protocol

- With respect to control frames, REP ALT port will block only tagged (part of Trunk EFP) control frames and not untagged (part of Untagged EFP) control frames.
- You must configure each segment port; an incorrect configuration can cause forwarding loops in networks.
- REP can manage only a single failed port within the segment; multiple port failures within the REP segment causes high loss of network connectivity.
- You should configure REP only in networks with redundancy. Configuring REP in a network without redundancy causes loss of network connectivity.
- Use LSL timers of 520mseconds to avoid REP flaps.
- The rate at which the layer 3 packets are punted to Host Q must be lesser than 1000 packets/second to avoid REP flap. The credit limit for Host Q is 1000 packets/second.
- There is no drop in REP LSL packet in STP Queue.
- REP is supported only on Trunk EFPs configured on the interfaces.
- REP enabled port do not support EFP configuration.

- The recommended minimum REP LSL timer value is 200 ms.
- The REP ports are removed from the topology list during the following situations:It is designed to avoid the traffic loop based on the above behavior to adopt dynamic REP configuration changes.
  - New port is added after the removal of the old port.
  - Both REP ports are removed.
  - The port is an Edge or Edge no neighbor port.
- A switch can support a maximum of 7 closed REP segments and 14 open REP segments.
- The recommended upper limit on the number of switches in a REP segment is 32.
- On a switch, a maximum of two ports can belong to a particular REP segment.
- REP enabled port do not support EFP configuration.
- SNMP trap for REP is not supported.

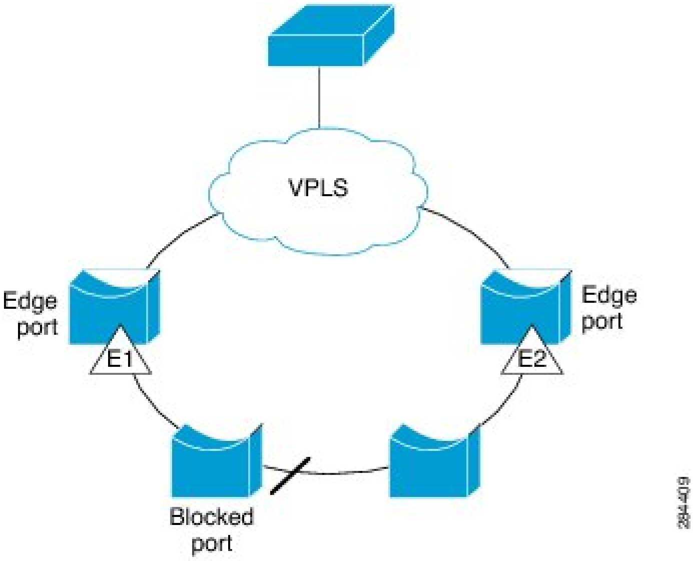
Information About REP

REP Segments

A REP segment is a chain of ports connected to each other and configured with a segment ID. Each segment consists of standard (nonedge) segment ports and two user-configured edge ports. A router 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 Ethernet Flow Point (EFP) interfaces.

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. When there is a failure in the network, the blocked port returns to the forwarding state to minimize network disruption.

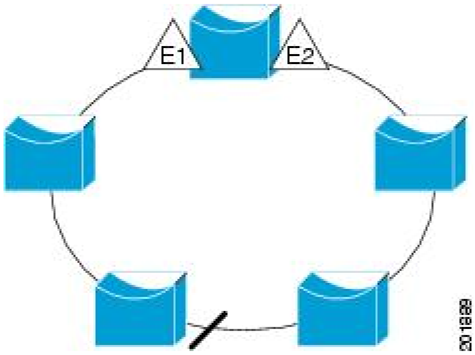
Figure 1: REP Open Segments



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 routers 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 all ports to ensure that connectivity is available through the other gateway.

The segment shown in the figure below is a ring segment, and it has both edge ports located on the same router. With this configuration, you can create a redundant connection between any two routers in the segment.

Figure 2: REP Ring Segment



REP segments have the following characteristics:

- If all ports in a segment are operational, one port (referred to as the *alternate* port) is in the blocked state for each VLAN. If VLAN load balancing is configured, two ports in the segment control the blocked state of VLANs.
- If one or more ports in a segment 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 up, 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. REP also supports VLAN load balancing, which is controlled by the primary edge port but can occurring at any port in the segment.

Link Integrity

REP does not use an end-to-end polling mechanism between edge ports to verify link integrity. It implements local link failure detection. When enabled on an interface, the REP Link Status Layer (LSL) detects its REP-aware neighbor and establishes connectivity within the segment. All VLANs are blocked on an interface until the REP LSL detects the neighbor. 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 up, LSL sends 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 under the following conditions:

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

Each port creates an adjacency with its immediate neighbor. Once the neighbor adjacencies are created, the ports negotiate to determine one blocked port for the segment, which is the alternate port. All other ports become unblocked. By default, REP packets are sent to a PortFast Bridge Protocol Data Unit (BPDU) class MAC address. The packets can also be sent to the Cisco multicast address, which at present is used only to send blocked port advertisement (BPA) messages when there is a failure in the segment. The packets are dropped by devices not running REP.

Fast Convergence

Because REP runs on a physical-link basis and not on a per-VLAN basis, only one hello message is required for all VLANs, thus reducing the load on the protocol. We recommend that you create VLANs consistently on all switches in a given segment and configure VLANs on 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 whole network, not just the REP segment. Switches that do not belong to the segment treat the messages as data traffic. You can control flooding of these messages by configuring a dedicated administrative VLAN for the whole domain.

The estimated convergence recovery time is less than 200 milliseconds (ms) for the local segment.

VLAN Load Balancing

One edge port in a REP segment acts as the primary edge port and the other as the secondary edge port. It is the primary edge port that always participates in VLAN load balancing in the segment. REP VLAN load balancing is achieved by blocking some VLANs at a configured alternate port and all other VLANs at the primary edge port. When you configure VLAN load balancing, you can specify the alternate port using any one of the following 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** command for the port.
- 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 You configure offset numbers on the primary edge port by identifying a port’s downstream position from the primary (or secondary) edge port. You cannot enter an offset value of 1 because 1 is the offset number of the primary edge port .

- By entering the **preferred** keyword to select the port that you previously configured as the preferred alternate port in the **rep segment preferred** command.

When the REP segment is complete, all VLANs are blocked. VLAN load balancing can be triggered in one of the following two ways:

- You can manually trigger VLAN load balancing at any time by entering the **rep preempt segment** *segment-id* command on the router that has the primary edge port.
- You can configure a preempt delay time by entering the **rep preempt delay** *seconds* command. After a link failure and recovery, VLAN load balancing begins after the configured preemption time period elapses. The delay timer restarts if another port fails before the time has elapsed.

Note A VLAN load balancing does not start working until triggered by either a 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 interfaces in the segment about the preemption. When the message is received by the secondary edge port, a message is generated in 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 VLANs. VLAN load balancing is initiated only by the primary edge port and 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.

To reconfigure VLAN load balancing, you must reconfigure the primary edge port. When you change the VLAN-load balancing configuration, the primary edge port again waits for the **rep preempt segment** command or for the configured preempt delay period after a port failure and recovery before executing the new VLAN load balancing 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 Protocol Interaction

REP does not interact with STP or with Flex Links but can coexist with both of them. 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 a 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 mean multiple blocked ports and a potential loss of connectivity. You can configure the edge ports when the segment has been configured in both directions up to the location of the edge ports.

REP Ports

Ports in REP segments take one of following three roles or states: Failed, Open, or Alternate.

- A port configured as a regular segment port starts as a failed port.
- After neighbor adjacencies are determined, the port transitions to the alternate port state, blocking all VLANs on the interface. Blocked port negotiations occur, and 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 ports move to the failed state. When the alternate port receives the failure notification, the port changes to the open state forwarding all 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 port is a designated blocking port. If the PortFast BPDU Guard Enhancement feature is configured or if STP is disabled, the port goes into the forwarding state.

Default REP Configuration

REP is disabled on all interfaces. When enabled, the interface is a regular segment port unless it is configured as an edge port.

When REP is enabled, the sending of segment topology change notices (STCNs) is disabled, all 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 VLANs at the primary edge port.

REP Segments and REP Administrative VLANs

A segment is a collection of ports connected in a chain and configured with a segment ID. To configure REP segments, you should configure the REP administrative VLAN (or use the default VLAN 1) and then add ports to the segment in interface configuration mode. You should configure two edge ports in the segment, with one as the primary edge port and the other, by default, as the secondary edge port. A segment has only one primary edge port. If you configure two ports in a segment as primary edge ports, for example, ports on different switches, REP selects one of them to serve as the primary edge port. You can also optionally configure where to send segment STCNs and VLAN load balancing. For more information about configuring REP Administrative VLANs, see the *Configuring the REP Administrative VLAN* section.

REP Configuration Guidelines

Follow these guidelines when configuring REP:

- We recommend that you begin by configuring one port and then configure contiguous ports to minimize the number of segments and the number of blocked ports.
- If more than two ports in a segment fail when no external neighbors are configured, one port goes into a forwarding state for the data path to help maintain connectivity during configuration. In the **show rep interface** command output, the Port Role for this port shows as “Fail Logical Open”; 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, 802.1ad or Trunk EFP 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 router if you enable REP in a Telnet session that accesses the router through the same interface.
- You cannot run REP and STP on the same segment or interface.
- If you connect an STP network to a REP segment, be sure that the connection is at the segment edge. An STP connection that is not at the edge could cause a bridging loop because STP does not run on REP segments. All STP BPDUs are dropped at REP interfaces.
- If REP is enabled on two ports on a router, both ports must be either regular segment ports or edge ports. REP ports follow these rules:
  - If only one port on a router is configured in a segment, the port should be an edge port.
  - If two ports on a router belong to the same segment, both ports must be edge ports or must be regular segment ports.
  - If two ports on a router 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 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 need to be aware of this status to avoid sudden connection losses.
- REP ports cannot be configured as one of the following port types:
  - Switched Port Analyzer (SPAN) destination port
  - Tunnel port
  - Access port
- There can be a maximum of two segments per port on the router. The maximum number of segments supported depends upon the number of ports available on the router.

REP Support on a Trunk EFP

Resilient Ethernet Protocol (REP) can be configured on Trunk EFP ports at the interface level on Cisco ASR 920 Series Router. Trunk EFP ports can have several bridged VLAN services running on them. Trunk EFP supports only 1000 VLANs. VLANs can be set to blocking and forwarding state on a Trunk EFP port. A user must enable REP on a port. By default, REP is disabled on all ports.

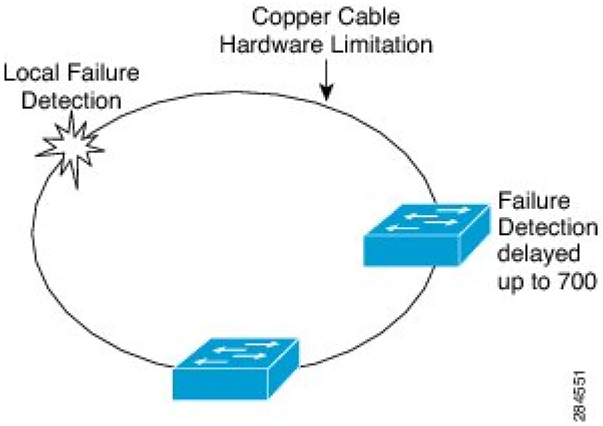
REP Configurable Timers

In a ring network topology, the Fast Last Link Status (LSL) process detects a neighboring port and maintains a connection with it. The timer on a port can be configured within 120-10000 ms to receive LSL frames. If no LSL frames are received from 120 to10000 ms from the neighboring port, the link between routers is considered as down. The tear-down operation and action is taken to bring up the link and restore traffic.

In the ring network topology, REP might fail to converge the traffic within 50 ms. For example, if the topology is made of copper cable, REP might fail to converge the traffic due to hardware limitations of the copper interface. In such a scenario, a remote end can take up to 700 ms to detect shutdown failure of a local port. The REP LSL is enhanced to achieve higher timer granularity and faster failure detection on the remote side.

The figure below shows the delay in failure detection due to hardware limitation of a Copper interface.

Figure 3: Delay in Failure Detection



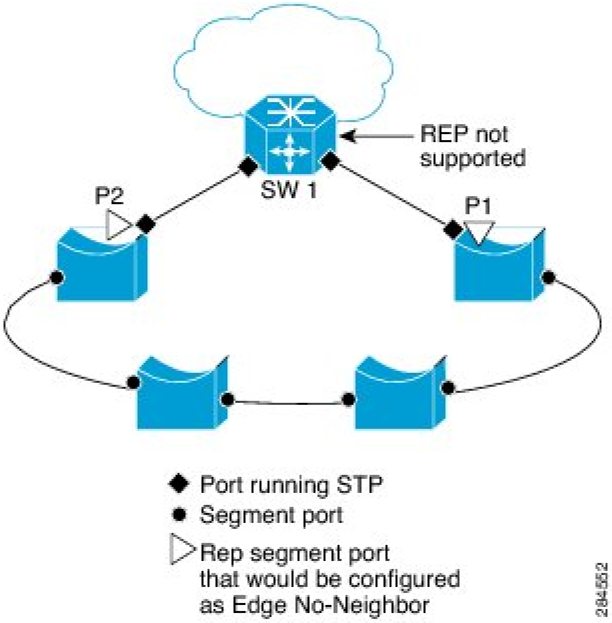
REP Edge No-Neighbor Support

In a ring network topology, aggregation nodes do not support REP. A REP segment can be created with no-neighbor ports to achieve convergence of switches. The figure below shows P1 and P2 as Edge No-Neighbor ports in a ring topology. In this configuration P1 and P2 can block traffic. If there is a failure on any of the links, all the switches with REP configuration converge. Since P1 and P2 are not edges, they do not support the following tasks:

- Perform VLAN load balancing.
- Detect topology changes to other segments and the Spanning Tree Protocol (STP).
- Choose the port that can preempt.
- Display the complete segment topology.

The Edge No-Neighbor support enables defining a new type of edge that has an internal neighbor. In the figure below, P1 and P2 are configured as Edge No-Neighbor ports rather than intermediate segment ports. These ports inherit properties of edge ports and overcome the limitations listed above. Thus, the Edge No-Neighbor port (P1 or P2) can send the Multiple Spanning Tree (MST) protocol, a Topology Change Notification (TCN), and a REP TCN for another segment towards the aggregation switch.

Figure 4: Ring Topology with Edge No-Neighbor Ports


REP not supported
SW 1
P2
P1
◆ Port running STP
● Segment port
▷ Rep segment port that would be configured as Edge No-Neighbor
284552

How to Configure REP

Configuring the REP Administrative VLAN

To avoid the delay introduced by relaying messages that are related to link-failures or VLAN-blocking notifications during VLAN load balancing, REP floods packets at the hardware flood layer (HFL) to a regular multicast address. These messages are flooded to the whole network and not just the REP segment. You can control flooding of these messages by configuring an administrative VLAN for the whole domain.

Follow these guidelines when configuring the REP administrative VLAN:

- There can be only one administrative VLAN on a router and on a segment. However, this is not enforced by the software.
- If you do not configure an administrative VLAN, the default is VLAN 1.
- If you want to configure REP on an interface, ensure that the REP administrative VLAN is part of the Trunk EFP encapsulation list.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **rep admin vlan** *vlan-id*
4. **end**
5. **show interface** [*interface-id*] **rep** [**detail**]
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**rep admin vlan** *vlan-id* **Example:** `Router(config)# rep admin vlan 2`	Configures a REP administrative VLAN. • Specify the administrative VLAN. The range is from 2 to 4094. The default is VLAN 1.

Step 4	**end**
	Example:
	`Router(config)# end`
		Returns to privileged EXEC mode.

Step 5	**show interface** [*interface-id*] **rep** [**detail**] **Example:** `Router# show interface gigabitethernet0/0/1 rep detail`	Displays the REP configuration and status for a specified interface. • Enter the physical interface or port channel ID.
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Save your entries in the router startup configuration file.

Configuring Trunk EFP on an Interface

Before you begin

For the REP operation, you must configure Trunk EFP on an interface. This task is required and must be done before configuring REP support on a Trunk EFP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **service instance trunk** *service-instance-id* **ethernet**
5. **encapsulation dot1q vlan** *range*
6. **rewrite ingress tag pop 1 symmetric**
7. **bridge-domain from-encapsulation**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet 0/0/1`	Specifies the interface, and enters interface configuration mode. • Enter the interface ID.
Step 4	**service instance trunk** *service-instance-id* **ethernet** **Example:** `Router(config-if)# service instance trunk 1 ethernet`	Configures a service instance on an interface and enters service instance configuration mode.
Step 5	**encapsulation dot1q vlan** *range* **Example:** `Router(config-if-srv)# encapsulation dot1q 1-20`	Defines the match criteria to be used to map dot1q frames ingress on an interface to the appropriate service instance. • The range of VLAN-IDs is from 1 to 4094.
Step 6	**rewrite ingress tag pop 1 symmetric** **Example:** `Router(config-if-srv)# rewrite ingress tag pop 1 symmetric`	Specifies the encapsulation adjustment to be performed on the frames ingress to the service instance.
Step 7	**bridge-domain from-encapsulation** **Example:** `Router(config-if-srv)# bridge-domain from-encapsulation`	Derives bridge domains from encapsulation.

	Command or Action	Purpose

Step 8	**end**
	Example:
	`Router (config-if-srv)end`
		Returns to privileged EXEC mode.

Configuring REP Support on a Trunk EFP

Before you begin

For the REP operation, you must enable REP on each segment interface and identify the segment ID. This task is required and must be done before other REP configurations. You must also configure a primary and secondary edge port on each segment. All other steps are optional.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface type number*
4. **rep segment** *segment-id* [**edge** [**primary**]] [**preferred**]
5. **rep stcn** {**interface** *type number* | **segment** *id-list* | **stp**}
6. **rep block port** {**id** *port-id* | *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**}
7. **rep preempt delay** *seconds*
8. **end**
9. **show interface** *type number* **rep** [**detail**]
10. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface type number* **Example:** `Router(config)# interface GigabitEthernet 0/0/1`	Specifies the interface and enters interface configuration mode. • Enter the interface type and number.
Step 4	**rep segment** *segment-id* [**edge** [**primary**]] [**preferred**] **Example:** `Router(config-if)# rep segment 3 edge preferred`	Enables REP on the interface and identifies a segment number. • The segment ID range is from 1 to 1024.

	Command or Action	Purpose
		Note You must configure two edge ports, including one primary edge port for each segment. • (Optional) **edge**—Configures the port as an edge port. Each segment has only two edge ports. Entering the **edge** without the **primary** keyword 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. **Note** Although each segment can have only one primary edge port, if you configure edge ports on two different switches and enter the **primary** keyword on both 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** privileged EXEC command. • (Optional) **preferred**—Indicates that the port is the preferred alternate port or the preferred port for VLAN load balancing. **Note** Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives the port a slight edge over equal contenders. The alternate port is usually a previously failed port.

Step 5	**rep stcn** {**interface** *type number* | **segment** *id-list* | **stp**}
	Example:
	`Router(config-if)# rep stcn segment 2-5`
		(Optional) Configures the edge port to send STCNs.
		• Use the **interface** *type number* keyword-argument pair to designate a physical interface or port channel to receive STCNs.
		• Use the **segment** *id-list* keyword-argument pair to identify one or more segments to receive STCNs. The range is from 1 to 1024.
		• Enter the**stp** to send STCNs to STP networks.

Step 6	**rep block port** {**id** *port-id* | *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**}
	Example:
	`Router(config-if)# rep block port 0009001818D68700 vlan all`
		(Optional) Configures VLAN load balancing on the primary edge port, identifies the REP alternate port in one of three ways, and configures the VLANs to be blocked on the alternate port.
		• Enter the **id** *port-id*keyword-pair to identify the alternate port by port ID. The port ID is automatically

	Command or Action	Purpose
		generated for each port in the segment. You can view interface port IDs by entering the **show interface** *type number* **rep** [**detail**] command. • Enter a *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 this command at the primary edge port (offset number 1), you cannot enter an offset value of 1 to identify an alternate port. • Enter the**preferred** keyword to select the regular segment port previously identified as the preferred alternate port for VLAN load balancing. • Enter the**vlan** *vlan-list* keyword-argument pair to block one VLAN or a range of VLANs. • Enter the**vlan all** keyword to block all VLANs. • Execute this command multiple times to accommodate the desired set of VLANs. It works as append VLAN to the existing list instead of replacing an existing one. **Note** Enter this command only on the REP primary edge port.
Step 7	**rep preempt delay** *seconds* **Example:** `Router(config-if)# rep preempt delay 60`	(Optional) Configures a preempt time delay. • Use this command if you want VLAN load balancing to automatically trigger 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** Use this command only on the REP primary edge port.

Step 8	**end**
	Example:
	`Router(config-if-srv)# end`
		Returns to privileged EXEC mode.

Step 9	**show interface** *type number* **rep** [**detail**] **Example:**	(Optional) Verifies the REP interface configuration.

	Command or Action	Purpose
	`Router# show interface Gigabitethernet0/0/1 rep detail`	• Enter the interface type and number and the optional **detail** keyword, if desired.
Step 10	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the router startup configuration file.

Setting the Preemption for VLAN Load Balancing

To set the preemption for VLAN load balancing, complete these steps on the router that has the segment with the primary edge port.

Restrictions

If you do not enter the **rep preempt delay** *seconds* command on the primary edge port to configure a preemption time delay, the default is to manually trigger VLAN load balancing on the segment. Use the **show rep topology** command to see which port in the segment is the primary edge port.

Before you begin

Be sure that all other segment configurations have been completed before setting the preemption for VLAN load balancing. When you enter the **rep preempt segment** *segment-id* command, a confirmation message appears before the command is executed because preemption for VLAN load balancing can disrupt the network.

SUMMARY STEPS

1. **enable**
2. **rep preempt segment** *segment-id*
3. **end**
4. **show rep topology**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**rep preempt segment** *segment-id* **Example:** `Router(config)# rep preempt segment 1`	Manually triggers VLAN load balancing on the segment. • Enter the segment ID. **Note** You will be asked to confirm the action before the command is executed.

	Command or Action	Purpose

Step 3	**end**
	Example:
	`Router(config)# end`
		Returns to privileged EXEC mode.

Step 4	**show rep topology** **Example:** `Router# show rep topology`	Displays the REP topology information.

Monitoring the REP Configuration

SUMMARY STEPS

1. **enable**
2. **show interface** [*interface-id*] **rep** [**detail**]
3. **show rep topology** [**segment** *segment-id*] [**archive**] [**detail**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show interface** [*interface-id*] **rep** [**detail**] **Example:** `Router# show interface gigabitethernet0/0/1 rep detail`	(Optional) Displays the REP configuration and status for a specified interface. • Enter the physical interface or port channel ID, and the optional **detail** keyword, if desired.
Step 3	**show rep topology** [**segment** *segment-id*] [**archive**] [**detail**] **Example:** `Router# show rep topology`	(Optional) Displays REP topology information for a segment or for all segments, including the primary and secondary edge ports in the segment. • Enter the optional keywords and arguments, as desired.

Configuring REP Configurable Timers

Before you begin

For the REP operation, you must enable REP on each segment interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **rep segment** *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**]
5. **rep stcn** {**interface** *type number* | **segment** *id-list* | **stp**}
6. **rep block port** {**id** *port-id* | *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**}
7. **rep lsl-retries** *number-of-tries*
8. **rep lsl-age-timer** *timer-value*
9. **rep preempt delay** *seconds*
10. **end**
11. **show interface** *type number* **rep** [**detail**]
12. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface Gigabitethernet 0/0/1`	Specifies the interface and enters interface configuration mode. • Enter the interface type and number.
Step 4	**rep segment** *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**] **Example:** `Router(config-if)# rep segment 1 edge preferred`	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. • (Optional) **edge**—Configures the port as an edge port. Each segment has only two edge ports. Entering the **edge** keyword without the **primary** keyword configures the port as the secondary edge port. • (Optional)**no-neighbor**—Configures the segment edge as one with no external REP neighbor on a port. • (Optional) **primary**—Configures the port as the primary edge port, the port on which you can configure VLAN load balancing.

	Command or Action	Purpose
		Note Although each segment can have only one primary edge port, if you configure edge ports on two different switches and enter the **primary** keyword on both 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** privileged EXEC command. • (Optional) **preferred**—Indicates that the port is the preferred alternate port or the preferred port for VLAN load balancing. **Note** Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives the port a slight edge over equal contenders. The alternate port is usually a previously failed port.

Step 5	**rep stcn** {**interface** *type number* | **segment** *id-list* | **stp**}
	Example:
	`Router(config-if)# rep stcn segment 2-5`
		(Optional) Configures the edge port to send STCNs.
		• Use the **interface** *type number* keyword and arguments pair to designate a physical interface or port channel to receive STCNs.
		• Use the **segment** *id-list* keyword and arguments pair to identify one or more segments to receive STCNs. The range is from 1 to 1024.
		• Enter the **stp** keyword to send STCNs to STP networks.

Step 6	**rep block port** {**id** *port-id* | *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**}
	Example:
	`Router(config-if)# rep block port 0009001818D68700 vlan all`
		(Optional) Configures VLAN load balancing on the primary edge port, identifies the REP alternate port in one of three ways, and configures VLANs to be blocked on the alternate port.
		• Enter the **id** *port-id* keyword and arguments pair to identify 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**] command.
		• Enter a *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.

	Command or Action	Purpose
		Note Because you enter this command at the primary edge port (offset number 1), you cannot enter an offset value of 1 to identify an alternate port. - Enter the **preferred** keyword to select the regular segment port previously identified as the preferred alternate port for VLAN load balancing. - Enter the **vlan** *vlan-list* keyword and arguments pair to block one VLAN or a range of VLANs. - Enter the **vlan all** keyword to block all VLANs. - Execute this command multiple times to accommodate the desired set of VLANs. It works as append VLAN to the existing list instead of replacing an existing one. **Note** Enter this command only on the REP primary edge port.
Step 7	**rep lsl-retries** *number-of-tries* **Example:** `Router(config-if)# rep lsl-retries 3`	Configures the number of retries permitted by LSL.
Step 8	**rep lsl-age-timer** *timer-value* **Example:** `Router(config-if)# rep lsl-age-timer 200`	Configures the failure detection time. - The valid range is from 120 to 10000.
Step 9	**rep preempt delay** *seconds* **Example:** `Router(config-if)# rep preempt delay 60`	- (Optional) Configures a preempt time delay. - Use this command if you want VLAN load balancing to automatically trigger after a link failure and recovery. - The time delay range is from 15 to 300 seconds. The default is manual preemption with no time delay. **Note** Use this command only on the REP primary edge port.

Step 10	**end**
	Example:
	`Router(config-if-srv)# end`
		Returns to privileged EXEC mode.

Step 11	**show interface** *type number* **rep** [**detail**] **Example:** `Router# show interface Gigabitethernet0/0/1 rep detail`	(Optional) Displays the REP interface configuration. - Enter the interface type and number and the optional **detail** keyword, if desired.

	Command or Action	Purpose
Step 12	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the router startup configuration file.

Configuring REP as an Edge No-Neighbor Port

Before you begin

For the REP operation, you must enable REP on each segment interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **rep segment** *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet 0/0/1`	Specifies the interface and enters interface configuration mode. • Enter the interface type and number.
Step 4	**rep segment** *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**] **Example:** `Router(config-if)# rep segment 1 edge no-neighbor preferred`	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. • (Optional) **edge**-Configures the port as an edge port. Each segment has only two edge ports. Entering **edge** without the **primary** keyword configures the port as the secondary edge port.

	Command or Action	Purpose
		• (Optional)**no-neighbor**-Indicates the segment edge as one with no external REP neighbor on a port. • (Optional) **primary**-Configures the port as the primary edge port, the port on which you can configure VLAN load balancing. **Note** Although each segment can have only one primary edge port, if you configure edge ports on two different switches and enter the **primary** keyword on both 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** privileged EXEC command. • (Optional) **preferred**-Indicates that the port is the preferred alternate port or the preferred port for VLAN load balancing. **Note** Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives the port a slight edge over equal contenders. The alternate port is usually a previously failed port.

Example

Configuration Examples for REP

Configuring the REP Administrative VLAN

This example shows how to configure the administrative VLAN as VLAN 100.

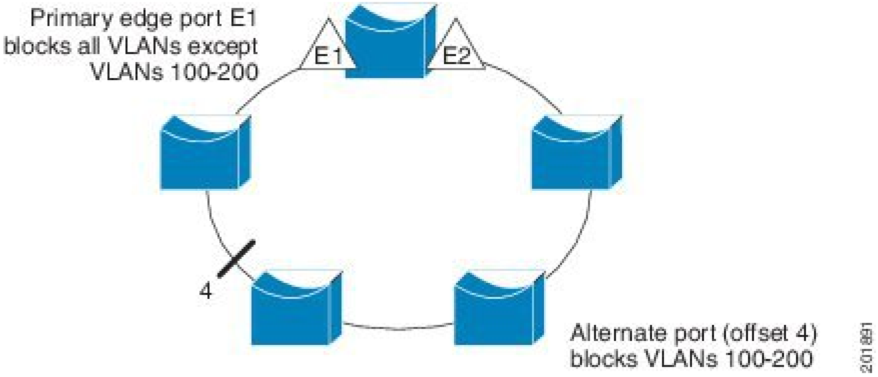
```
Router# configure terminal
Router(config)# rep admin vlan 100
Router(config-if)# end
```

Configuring REP Support on a Trunk EFP

This example shows how to configure REP support on a Trunk EFP. An interface is configured as the primary edge port for segment 1 to send STCNs to segments 2 through 5; the alternate port is configured as the port with port ID 0009001818D68700 to block all VLANs after a preemption delay of 60 seconds after a segment port failure and recovery.

```
Router# configure terminal
Router(config)# interface gigabitethernet0/0/1
Router(config-if)# rep segment 1 edge primary
Router(config-if)# rep stcn segment 2-5
Router(config-if)# rep block port id 0009001818D68700 vlan all
Router(config-if)# rep preempt delay 60
Router(config-if)# service instance trunk 1 ethernet
Router(config-if-srv)# encapsulation dot1q 10-20
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain from-encapsulation
Router(config-if-srv)# end
```

This example shows how to configure the VLAN blocking configuration as shown in the figure below. The alternate port is the neighbor with neighbor offset number 4. After manual preemption, VLANs 100 to 200 are blocked at this port and all other VLANs are blocked at the primary edge port E1 (Gigabit Ethernet port 0/0/1).


Primary edge port E1 blocks all VLANs except VLANs 100-200
E1
E2
4
Alternate port (offset 4) blocks VLANs 100-200
201891

```
Router# configure terminal
Router(config)# interface gigabitethernet0/0/1
Router(config-if)# rep segment 1 edge primary
Router(config-if)# rep block port 4 vlan 100-200
Router(config-if)# end
```

Setting the Preemption for VLAN Load Balancing

```
Router>end
Router# preempt segment 1000
The command will cause a momentary traffic disruption. Do you still want to continue?

[confirm]Proceeding with Manual Preemption
```

Configuring SNMP Traps for REP

This example shows how to configure the router to send REP traps at a rate of 10 traps per second:

```
Router> enable
Router# configure terminal
Router(config)# snmp mib rep trap-rate 10
Router(config)# end
```

Monitoring the REP Configuration

The following is sample output of the **show interface rep detail** command. Use the **show interface rep detail** command on one of the REP interfaces to monitor and verify the REP configuration.

```
Router# show interface GigabitEthernet 0/0/1 rep detail

GigabitEthernet0/0/1 REP enabled
Segment-id: 2 (Edge)
PortID: 00010019E7144680
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 0002001121A2D5800E4D
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 100
Preempt Delay Timer: disabled
Load-balancing block port: none
Load-balancing block vlan: none
STCN Propagate to: none
LSL PDU rx: 3322, tx: 1722
HFL PDU rx: 32, tx: 5
BPA TLV rx: 16849, tx: 508
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 118, tx: 118
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 4214, tx: 4190
```

Configuring REP Configurable Timers

```
Router# configure terminal
Router(config)# interface GigabitEthernet 0/0/4
Router(config-if)# rep segment 4 edge preferred
Router(config-if)# rep stcn segment 2-5
Router(config-if)# rep block port 0009001818D68700 vlan all
Router(config-if)# rep lsl-retries 3
Router(config-if)# rep lsl-age-timer 200
Router(config-if)# rep preempt delay 300
Router(config-if)# exit
Router# show interface GigabitEthernet 0/0/1 rep detail
Router# copy running-config startup-config
```

Configuring REP Edge No-Neighbor Support

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet0/0/2
Router(config-if)# rep segment 4 edge no-neighbor primary
```

CHAPTER 2

REP Access Gateway

Resilient Ethernet Protocol (REP) is a ring protection protocol designed to provide fast failure detection and recovery. A REP Edge No-Neighbor (RENN) port is a port at the edge of a REP segment, connected to a peer device that does not support REP. This feature allows CFM to notify REP when an error is detected, such that CFM can be used to monitor the status of the Edge link, and REP can take actions.

This feature allows communication for REP to enable Ethernet Fault Detection (EFD) notifications between the routers configured with REP Access Gateway (REP-AG).

Prerequisites for REP Access Gateway

- The interface connected to non-REP device port should be configured as a REP edgeNN port.
- CCM notification is processed only on a REP edgeNN port.
- Port MEP is only supported in REP AG. Port MEPs are configured to protect a single hop and used to monitor link state through CFM. See Configuring Ethernet Connectivity Fault Management in a Service Provider Network.
- EFD is supported on down MEPs. A down MEP sends and receives CFM frames through the wire connected to the port on which the MEP is configured. See Configuring Ethernet Connectivity Fault Management in a Service Provider Network.

Restrictions for REP Access Gateway

- REP AG is supported for only for Port MEPs.
- When a link down is observed between the REP and Non-REP device, the convergence time is greater with a Copper connection.

- EFD is supported on Port MEPs and EFP MEPs.
- CCM interval for MAs on which EFD is supported is limited.
- EFD is *not* supported on Trunk EFPs.
- EFD notifications are only supported for a single client per MA. EFD notifications are *not* supported for both G-8032 and REP simultaneously.
- Only a single MEP can be configured on a the interface or EFP for EFD.
- REP Edge No-Neighbour (ENN) configured ports receiving Link Status Layer (LSL) frames from the peer node will automatically be converted to REP ports.

  You will see the log message **%REP-6-AUTOCONFIG: Interface GigabitEthernet< >** automatically configured to the REP device.
- REP is supported on port-channel interface, without **efd notify rep** (CCM).
- The convergence time is between 100miliseconds to 200miliseconds.

Information About REP Access Gateway

In a network when a link failure occurs, a Non-REP device network (access gateway) directly connected to REP network sends failure notification, so that REP network can reroute the traffic to alternate route. But, access devices supporting REP Edge No-Neighbor (REP ENN) only support one interface configured as a REP Edge No-Neighbor port resulting in an unsupported architecture with the REP Access Gateway (REP AG) device.

Fast failure detection can be established by enabling communication between Connectivity Fault Manager (CFM) and REP. CFM on the edge ports can notify REP if any failures are detected on the monitored links, allowing the appropriate re-convergence actions to be taken.

The mechanism for the communication is for REP to register as an Ethernet Fault Detection (EFD) client, so that any CFM defects above a configurable threshold triggers a notification to REP.

Note To trigger EFD notifications on the router, CFM must be configured.

REP Access Gateway Enhancements

In a network where a REP and non-REP devices are connected and when a link failure occurs, a Non-REP device network (access gateway) directly connected to REP network sends failure notification, so that REP network can reroute the traffic to an alternate route. But, access devices supporting REP Edge No-Neighbor (REP ENN) only support one interface configured as a REP Edge No-Neighbor port, resulting in an unsupported architecture with the REP Access Gateway (REP AG) device.

Fast failure detection in a REP-AG configured device can be achieved by enabling communication between Connectivity Fault Manager (CFM) and REP. CFM on the edge ports can notify REP if any failure is detected on the monitored links, allowing the appropriate re-convergence actions to be taken.

The mechanism for the communication is for REP to register as an Ethernet Fault Detection (EFD) client, so that any CFM defects above a configurable threshold triggers a notification to REP.

How to Configure REP Access Gateway

Enabling EFD Notifications

Before you begin

CFM IEEE must be enabled before enabling EFD notifications. For information, see Configuring Ethernet Connectivity Fault Management in a Service Provider Network.

For information on CFM configuration, see the Carrier Ethernet Configuration Guide, Cisco IOS XE Release (Cisco NCS 520).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **service** {*short-ma-name* | **number** *MA-number* | **vlan-id** *primary-vlan-id* | **vpn-id** *vpn-id*} {**vlan** *vlan-id* | **port** | **evc** *evc-name*} **direction** {**up** | **down**}
5. **continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**]
6. **continuity-check** [**interval** *cc-interval*]
7. **efd notify** {**g8032** | **rep**}
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Router(config)# ethernet cfm domain Customer level 7`	Defines a CFM maintenance domain at a specified maintenance level and places the CLI in Ethernet CFM configuration mode.

	Command or Action	Purpose

Step 4	**service** {*short-ma-name* | **number** *MA-number* | **vlan-id** *primary-vlan-id* | **vpn-id** *vpn-id*} {**vlan** *vlan-id* | **port** | **evc** *evc-name*} **direction** {**up** | **down**}
	Example:
	`Device(config-ecfm)# service s1 port`
		Configures a maintenance association within a maintenance domain and enters Ethernet connectivity fault management (CFM) service configuration mode.

Step 5	**continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**] **Example:** `Router(config-ecfm-srv)# continuity-check`	Enables the transmission of CCMs.
Step 6	**continuity-check** [**interval** *cc-interval*] **Example:** `Device(config-ecfm-srv)# continuity-check interval 10s`	Configures the per-service parameters and sets the interval at which CCMs are transmitted.

Step 7	**efd notify** {**g8032** | **rep**}
	Example:
	`Router(config)# **efd notify rep**`
		• **g8032**—Enables G.8032 notifications on the MA.
		• **rep**—Enables REP notifications on the MA.
		.
		Note Either g8032 or rep notifications can be configured for an MA at an instance. For example, if REP notifications are enabled while G.8032 notifications are enabled for an MA, the G.8032 notifications are disabled.

Step 8	**end**
	Example:
	`Router# **end**`
		Returns to privileged EXEC mode.

Configuration Examples

Example: Configuring REP AG EFD

The example shows EFD notify enabled on the router.

```
ethernet cfm ieee
ethernet cfm global
ethernet cfm traceroute cache
ethernet cfm traceroute cache hold-time 60
ethernet cfm domain d1 level 6
 service s1 port
  continuity-check
  continuity-check interval 100ms
  efd notify rep
end
..
1


interface GigabitEthernet0/1/2
ethernet cfm mep domain d1 mpid 3 service s1
 service instance trunk 1 ethernet
  encapsulation dot1q 209-212
  rewrite ingress tag pop 1 symmetric
  bridge-domain from-encapsulation
end
..
!


interface GigabitEthernet0/1/3
ethernet cfm mep domain d1 mpid 4 service s1
 service instance trunk 1 ethernet
  encapsulation dot1q 209-212
  rewrite ingress tag pop 1 symmetric
  bridge-domain from-encapsulation
end
..
!
```

Verifying REP Access Gateway

Example: Verifying REP AG EFD Notifications

Use the **show interface** command to view the status EFD.

- This example shows EFD status on the interface .

```
Router# show interface gigabitethernet 0/1/7 rep detail

 Interface Gi0/1/7
---
GigabitEthernet1/7   REP enabled

Segment-id: 1 (Primary Edge No-Neighbor)
PortID: 000DE8BA70DD3000
Preferred flag: No
Operational Link Status: NO_NEIGHBOR
Current Key: 001878DA6ED817002FF3
Port Role: Open
Blocked VLAN: empty
Admin-vlan: 2
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: STP
EFD State : Enabled
EFD Status : Clear
LSL PDU rx: 0, tx: 0
HFL PDU rx: 32, tx: 1
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: 18
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 0, tx: 0
```

- This example shows REP topology.

```
Router# show rep topolgy

REP Segment 911
BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
node3            Te0/0/12   Pri* Alt
node3            Gi0/0/11        Open
node4            Gi0/0/11        Open
node4            Gi0/0/0         Open
node2            Gi0/0/0         Open
node2            Gi0/0/7    Sec* Open
```

- This example shows the CFM EFD MEP information.

Note Configure service internal in configuration mode before executing the **show ethernet cfm efd mep** command.

```
Router# show ethernet cfm efd mep

Domain d1, Service s1: notify REP, EFD not triggered
    ID Interface  SrvcInst Defect        Threshold     Triggered?
    ---- ---------- -------- ------------- ------------- ----------
     4 Te0/0/12   N/A      None          DefMACstatus  No
```

This example shows the CFM EFD MEP information when a fault is detected.

```
Router# show ethernet cfm efd meps | sec ring1
Domain dom1_ring1, Service ser1_ring1: notify REP, EFD not triggered
ID    Interface  SrvcInst   Defect     Threshold   Triggered?
----  ---------  --------   -------    ---------  ----------
3     Te0/0/12    NA        None      DefMACstatus  No
```

CHAPTER 3

UniDirectional Link Detection (UDLD) Protocol

The UniDirectional Link Detection protocol is a Layer 2 protocol that detects and disables one-way connections before they create undesired situation such as Spanning Tree loops.

Restrictions for the UDLD Protocol

- Only Gigabit Ethernet and TenGigabit Ethernet are supported.
- Supports only the basic UDLD functions.

Information About the UDLD Protocol

UDLD Overview

The Cisco-proprietary UDLD protocol allows the devices connected through fiber optic or copper (for example, Category 5 cabling) Ethernet cables that are connected to the LAN ports to monitor the physical configuration of the cables and detect whether a unidirectional link exists. When a unidirectional link is detected, the UDLD shuts down the affected LAN port and alerts the corresponding user, because unidirectional links cause a variety of problems, including spanning tree topology loops.

UDLD is a Layer 2 protocol that works with the Layer 1 protocols to determine the physical status of a link. In Layer 1, auto negotiation takes care of physical signaling and fault detection. UDLD performs tasks that auto negotiation cannot perform, such as detecting the identities of neighbors and shutting down misconnected LAN ports. When you enable both auto negotiation and UDLD, the Layer 1 and Layer 2 detections work together to prevent physical and logical unidirectional connections and the malfunctioning of other protocols.

A unidirectional link occurs whenever the traffic transmitted by a local device over a link is received by a neighbor, but traffic transmitted from the neighbor is not received by the local device. If one of the fiber strands in a pair is disconnected, the link does not stay up as long as the auto negotiation is active. In such a scenario, the logical link is undetermined, and the UDLD does not take any action. If both the fibers are working normally in Layer 1, the UDLD in Layer 2 determines whether those fibers are connected correctly and whether the traffic is flowing bidirectionally between the correct neighbors. This check cannot be performed by auto negotiation because auto negotiation operates in Layer 1.

The router periodically transmits the UDLD packets to the neighbor devices on LAN ports where UDLD is enabled. If the packets are echoed back within a specific timeframe and they are lacking a specific acknowledgment (echo), the link is flagged as unidirectional and the LAN port is shut down. Devices on both ends of the link must support UDLD for the protocol to successfully identify and disable the unidirectional links.

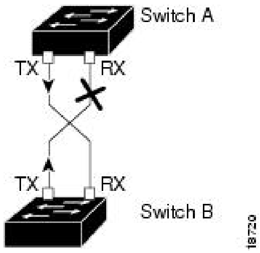
UDLD detects and disables unidirectional links on Ethernet fiber and copper interfaces due to miswiring or malfunctioning of the interfaces.

Note UDLD is disabled by default on all ports to avoid sending unnecessary traffic.

To configure fibre-optic interfaces, enable the **udld** command at the global level. For copper interfaces, enable the **udld port** command at the interface level.

The figure displays the UDLD mechanism.

Figure 5: Unidirectional Link



UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD can detect unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD can also detect unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and to misconnected interfaces on fiber-optic links.

UDLD Normal Mode

In normal mode, UDLD detects the unidirectional link when fiber strands in a fiber-optic interface are misconnected and the Layer 1 mechanisms do not detect this misconnection. If the interfaces are connected correctly, but the traffic is one way, UDLD does not detect the unidirectional link because the Layer 1 mechanism, which is supposed to detect this condition, does not do so. In case, the logical link is considered undetermined, and UDLD does not disable the interface. If one of the fiber strands in a pair is disconnected and autonegotiation is active, the link does not stay up because the Layer 1 mechanisms did not detect a physical problem with the link. In this case, UDLD does not take any action, and the logical link is considered undetermined.

UDLD Aggressive Mode

The UDLD aggressive mode is configured only on the point-to-point link between the network devices that support the UDLD aggressive mode. With UDLD aggressive mode enabled, a port on a bidirectional link that has a UDLD neighbor relationship established stops receiving the UDLD packets. The UDLD tries to re-establish the connection with the neighbor; the port is disabled after eight failed retries.

To prevent spanning tree loops, nonaggressive UDLD with the default interval of 15 seconds is fast enough to shut down a unidirectional link before a blocking port transitions to the forwarding state (with default spanning tree parameters).

The UDLD can error disable the ports on the link to prevent the traffic from being discarded under the following scenarios, when either of the modes is enabled. That is normal or aggressive mode:

- One side of a link has a port (either Tx and Rx) stuck.
- One side of a link remains up while the other side of the link has gone down.

UDLD Functions

UDLD performs the following functions

- Sends a probe packet on every active interface on which UDLD is configured to keep each device informed about its neighbors.
- Learns about the neighbors and keeps the updated neighbor information in a cache table
- Sends several echo messages whenever it detects a new neighbor sending UDLD packets or whenever a neighbor requests a resynchronization of the caches
- Shuts down the affected port and notifies the user when one-way connection is detected. Devices on both ends of the link must support UDLD in order for the protocol to successfully identify and disable unidirectional links
- Reestablishes the connection with the neighbor when a port on a bidirectional link stops receiving UDLD packets if aggressive mode is enabled. After eight failed retries, the port goes into disabled state

Detecting Unidirectional Links

UDLD operates by using two mechanisms:

Neighbor database maintenance

UDLD learns about other UDLD-capable neighbors by periodically sending a hello packet (also called an advertisement or probe) on every active interface to keep each device informed about its neighbors. When the switch receives a hello message, it caches the information until the age time (hold time or time-to-live) expires. If the switch receives a new hello message before an older cache entry ages, the switch replaces the older entry with the new one. Whenever an interface is disabled and UDLD is running, whenever UDLD is disabled on an interface, or whenever the switch is reset, UDLD clears all existing cache entries for the interfaces affected by the configuration change. UDLD sends at least one message to inform the neighbors to flush the part of their caches affected by the status change. The message is intended to keep the caches synchronized.

Event-driven detection and echoing

UDLD relies on echoing as its detection mechanism. Whenever a UDLD device learns about a new neighbor or receives a resynchronization request from an out-of-sync neighbor, it restarts the detection window on its side of the connection and sends echo messages in reply. Because this behavior is the same on all UDLD neighbors, the sender of the echoes expects to receive an echo in reply. If the detection window ends and no valid reply message is received, the link might shut down, depending on the UDLD mode. When UDLD is in normal mode, the link might be considered undetermined and might not be shut down. When UDLD is in aggressive mode, the link is considered unidirectional, and the interface is shut down. If UDLD in normal mode is in the advertisement or in the detection phase and all the neighbor cache entries are aged out, UDLD restarts the link-up sequence to resynchronize with any potentially out-of-sync neighbors. If you enable aggressive mode when all the neighbors of a port have aged out either in the advertisement or in the detection phase, UDLD restarts the link-up sequence to resynchronize with any potentially out-of-sync neighbor. UDLD shuts down the port if, after the fast train of messages, the link state is still undetermined.

How to Configure UDLD Protocol

Enabling UDLD Protocol

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **udld** {**enable** | **aggressive**}
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 3	**udld** {**enable**	**aggressive**}
		Example:
		`Router(config)# udld enable`
			Enables UDLD protocol on the router.

Step 4	**end**
	Example:
	`Router# end`
		Returns to privileged EXEC mode.

Enabling UDLD Protocol at Interface Level

SUMMARY STEPS

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

4. **udld port** [**aggressive**]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Router(config)# interface gigabitethernet0/0/1`	Enter interface configuration mode. Valid interfaces are physical ports.
Step 4	**udld port** [**aggressive**] **Example:** `Router(config)# udld port aggressive`	Enables UDLD on a specific port. Enter the aggressive keyword to enable the aggressive mode. On a fiber-optic LAN port, this command overrides the udld enable global configuration command setting. Use the **no** form of this command to disable the UDLD on a non fiber-optic LAN port.

Step 5	**end**
	Example:
	`Router# end`
		Returns to privileged EXEC mode.

Enabling UDLD Protocol at Interface Level

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **udld port** [**aggressive**]
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Router(config)# interface gigabitethernet0/0/1`	Enter interface configuration mode. Valid interfaces are physical ports.
Step 4	**udld port** [**aggressive**] **Example:** `Router(config)# udld port aggressive`	Enables UDLD on a specific port. Enter the aggressive keyword to enable the aggressive mode. On a fiber-optic LAN port, this command overrides the udld enable global configuration command setting. Use the **no** form of this command to disable the UDLD on a non fiber-optic LAN port.

Step 5	**end**
	Example:
	`Router# end`
		Returns to privileged EXEC mode.

Enabling UDLD Probe Message Interval

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **udld message time** *interval*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**udld message time** *interval* **Example:** `Router(config)# udld message time 90`	Set the time in seconds between UDLD probe messages. The valid range is from 7 to 90 seconds. The default is 15 seconds

	Command or Action	Purpose

Step 4	**end**
	Example:
	`Router# end`
		Returns to privileged EXEC mode.

Recovering the UDLD Protocol

UDLD recovery when enabled, attempts to bring an UDLD error-disabled port out of reset. Tthe default recovery timer is 300 seconds.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **udld recovery** *inteval*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**udld recovery** *inteval* **Example:** `Router(config)# udld recovery`	Enables UDLD recovery on the router. • *inteval*—Sets the recovery time interval. The valid range is from 30 to 86400 seconds. The default value is 300 seconds.

Step 4	**end**
	Example:
	`Router# end`
		Returns to privileged EXEC mode.

Resetting Ports

SUMMARY STEPS

1. **enable**
2. **udld reset**
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**udld reset** **Example:** `Router# udld reset`	Resets ports that are shut down by UDLD.

Step 3	**end**
	Example:
	`Router# end`
		Returns to privileged EXEC mode.

Configuration Examples

Example: Configuring UDLD Protocol

This example shows UDLD on the router.

```
show running-config | i udld
udld enable
udld message time 7
udld recovery
udld recovery interval 30
```

Verifying UDLD Protocol

Example: Verifying UDLD Protocol

Use the **show udld** command to view the status of the UDLD protocol on the ports.

- This example shows UDLD protocol on all ports the router.

```
Router# show udld
 Interface Te0/0/0
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 15
Time out interval: 5

    Entry 1
    ---
    Expiration time: 40
    Cache Device index: 1
    Current neighbor state: Bidirectional
    Device ID: FOX1736P0JP
    Port ID: Te0/1/0
    Neighbor echo 1 device: FOX1709P3D0
    Neighbor echo 1 port: Te0/0/0

    Message interval: 15
    Time out interval: 5
    CDP Device name: RSP1B

Interface Gi0/2/0
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 15
Time out interval: 5

    Entry 1
    ---
    Expiration time: 33
    Cache Device index: 1
    Current neighbor state: Bidirectional
    Device ID: FOC1528V27K
    Port ID: Gi0/2
    Neighbor echo 1 device: FOX1709P3D0
    Neighbor echo 1 port: Gi0/2/0

    Message interval: 15
    Time out interval: 5
    CDP Device name: RSP1A

Interface Gi0/2/1
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 15
Time out interval: 5

    Entry 1
    ---
    Expiration time: 33
    Cache Device index: 1
    Current neighbor state: Bidirectional
    Device ID: FOC1639V1Z4
    Port ID: Gi0/4
    Neighbor echo 1 device: FOX1709P3D0
    Neighbor echo 1 port: Gi0/2/1

    Message interval: 15
    Time out interval: 5
    CDP Device name: RSP1A

Interface Gi0/2/2
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Unknown
Current operational state: Advertisement
Message interval: 15
Time out interval: 5
```

```
No neighbor cache information stored

Interface Gi0/2/3
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Unknown
Current operational state: Link down
Message interval: 15
Time out interval: 5
No neighbor cache information stored

Interface Gi0/2/4
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Gi0/2/5
---
Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Gi0/2/6
---
Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown
.
.
.
```

- This example shows UDLD protocol on the Ten Gigabit Ethernet interface.

```
Router# show udld tengigabitethernet 0/0/0

Interface Te0/0/0
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 15
Time out interval: 5

    Entry 1
    ---
    Expiration time: 43
    Cache Device index: 1
    Current neighbor state: Bidirectional
    Device ID: FOX1736P0JP
    Port ID: Te0/1/0
    Neighbor echo 1 device: FOX1709P3D0
    Neighbor echo 1 port: Te0/0/0

    Message interval: 15
    Time out interval: 5
    CDP Device name: RSP1B

Router# show running-config | i udld
udld enable
udld message time 15
udld recovery
udld recovery interval 30
```

- This example shows the UDLD protocol neighbors.

```
Router# show udld neighbors

Port          Device Name     Device ID     Port ID        Neighbor State
------------ ------------- ------------ ------------ ----------------
Te0/0/0         FOX1736P0JP     1            Te0/1/0         Bidirectional
Gi0/2/0         FOC1528V27K     1            Gi0/2           Bidirectional
Gi0/2/1         FOC1639V1Z4     1            Gi0/4           Bidirectional
```

CHAPTER 4

ITU-T G.8032 Ethernet Ring Protection Switching

The ITU-T G.8032 Ethernet Ring Protection Switching feature implements protection switching mechanisms for Ethernet layer ring topologies. This feature uses the G.8032 Ethernet Ring Protection (ERP) protocol, defined in ITU-T G.8032, to provide protection for Ethernet traffic in a ring topology, while ensuring that no loops are within the ring at the Ethernet layer. The loops are prevented by blocking traffic on either a predetermined link or a failed link.

Prerequisites for Configuring ITU-T G.8032 Ethernet Ring Protection Switching

- Trunk Ethernet Flow Points (TEFPs) must be configured under the interface.

About ITU-T G.8032 Ethernet Ring Protection Switching

Ring Protection Links

An Ethernet ring consists of multiple Ethernet ring nodes. Each Ethernet ring node is connected to adjacent Ethernet ring nodes using two independent ring links. A ring link prohibits formation of loops that affect the network. The Ethernet ring uses a specific link to protect the entire Ethernet ring. This specific link is called the Ring Protection Link (RPL). A ring link is bound by two adjacent Ethernet ring nodes and a port for a ring link (also known as a ring port). There must be at least two Ethernet ring nodes in a Ethernet ring.

ITU-T G.8032 Ethernet Ring Protection Switching Functionality

The Ethernet ring protection functionality includes the following:

- Loop avoidance

- The use of learning, forwarding, and Filtering Database (FDB) mechanisms

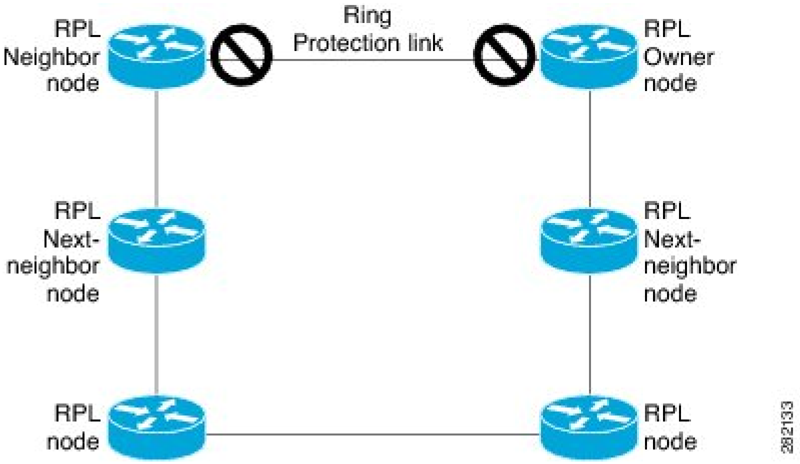
Loop avoidance in an Ethernet ring is achieved by ensuring that, at any time, traffic flows on all but the Ring Protection Link (RPL).

The following is a list of RPL types (or RPL nodes) and their functions:

- RPL owner—Responsible for blocking traffic over the RPL so that no loops are formed in the Ethernet traffic. There can be only one RPL owner in a ring.
- RPL neighbor node—An Ethernet ring node adjacent to the RPL. It is responsible for blocking its end of the RPL under normal conditions. This node type is optional and prevents RPL usage when protected.
- RPL next-neighbor node—Next-neighbor node is an Ethernet ring node adjacent to an RPL owner node or RPL neighbor node. It is mainly used for FDB flush optimization on the ring. This node is also optional.

The following figure illustrates the G.8032 Ethernet ring topology.

Figure 6: G.8032 Ethernet Ring Topology



R-APS Control Messages

Nodes on the ring use control messages called Ring Automatic Protection Switching (R-APS) messages to coordinate the activities of switching the ring protection link (RPL) on and off. Any failure along the ring triggers a R-APS Signal Failure (R-APS SF) message in both directions of the nodes adjacent to the failed link, after the nodes have blocked the port facing the failed link. On obtaining this message, the RPL owner unblocks the RPL port.

Note A single link failure in the ring ensures a loop-free topology.

CFM Protocols and Link Failures

Connectivity Fault Management (CFM) and line status messages are used to detect ring link and node failure. During the recovery phase, when the failed link is restored, the nodes adjacent to the restored link send Ring Automatic Protection Switching (R-APS) No Request (R-APS NR) messages. On obtaining this message, the ring protection link (RPL) owner blocks the RPL port and sends R-APS NR and R-APS RPL (R-APS NR, RB) messages. These messages cause all other nodes, other than the RPL owner in the ring, to unblock all blocked ports. The Ethernet Ring Protection (ERP) protocol works for both unidirectional failure and multiple link failure scenarios in a ring topology.

Note The G.8032 Ethernet Ring Protection (ERP) protocol uses CFM Continuity Check Messages (CCMs) at an interval of 3.3 milliseconds (ms). At this interval (which is supported only on selected platforms), SONET-like switching time performance and loop-free traffic can be achieved.

G.8032 Ring-Supported Commands and Functionality

A G.8032 ring supports these basic operator administrative commands:

- Force switch (FS)—Allows the operator to forcefully block a particular ring port. Note the following points about FS commands:
  - Effective even if there is an existing SF condition
  - Multiple FS commands for ring are supported
  - May be used to allow immediate maintenance operations
- Manual switch (MS)—Allows the operator to manually block a particular ring port. Note the following points about MS commands:
  - Ineffective in an existing FS or signal failure (SF) condition
  - Overridden by new FS or SF conditions
  - When multiple MS commands are executed more than once on the same device, all MS commands are cancelled.

    When multiple MS commands are executed on different devices in the ring, for the same instance, then the command executed on the second device is rejected.
- Clear—Cancels an existing FS or MS command on the ring port. The Clear command is used at the ring protection link (RPL) owner to clear a nonrevertive mode condition.

A G.8032 ring can support multiple instances. An instance is a logical ring running over a physical ring. Such instances are used for various reasons, such as load-balancing VLANs over a ring. For example, odd-numbered VLANs may go in one direction of the ring, and even-numbered VLANs may go in the other direction. Specific VLANs can be configured under only one instance. They cannot overlap multiple instances. Otherwise, data traffic or Ring Automatic Protection Switching (R-APS) messages may cross logical rings, which is not desirable.

G.8032 ERP Timers

The G.8032 Ethernet Ring Protection (ERP) protocol specifies the use of different timers to avoid race conditions and unnecessary switching operations:

- Delay timers—Used by the Ring Protection Link (RPL) owner to verify that the network has stabilized before blocking the RPL. Note the following points about delay timers.
  - After a signal failure (SF) condition, a Wait-to-Restore (WTR) timer is used to verify that the SF is not intermittent.
  - The WTR timer can be configured by the operator. The default time interval is 5 minutes; the time interval ranges from 1 to 12 minutes.
  - After a force switch (FS) or a manual switch (MS) command is issued, a Wait-to-Block (WTB) timer is used to verify that no background condition exists.

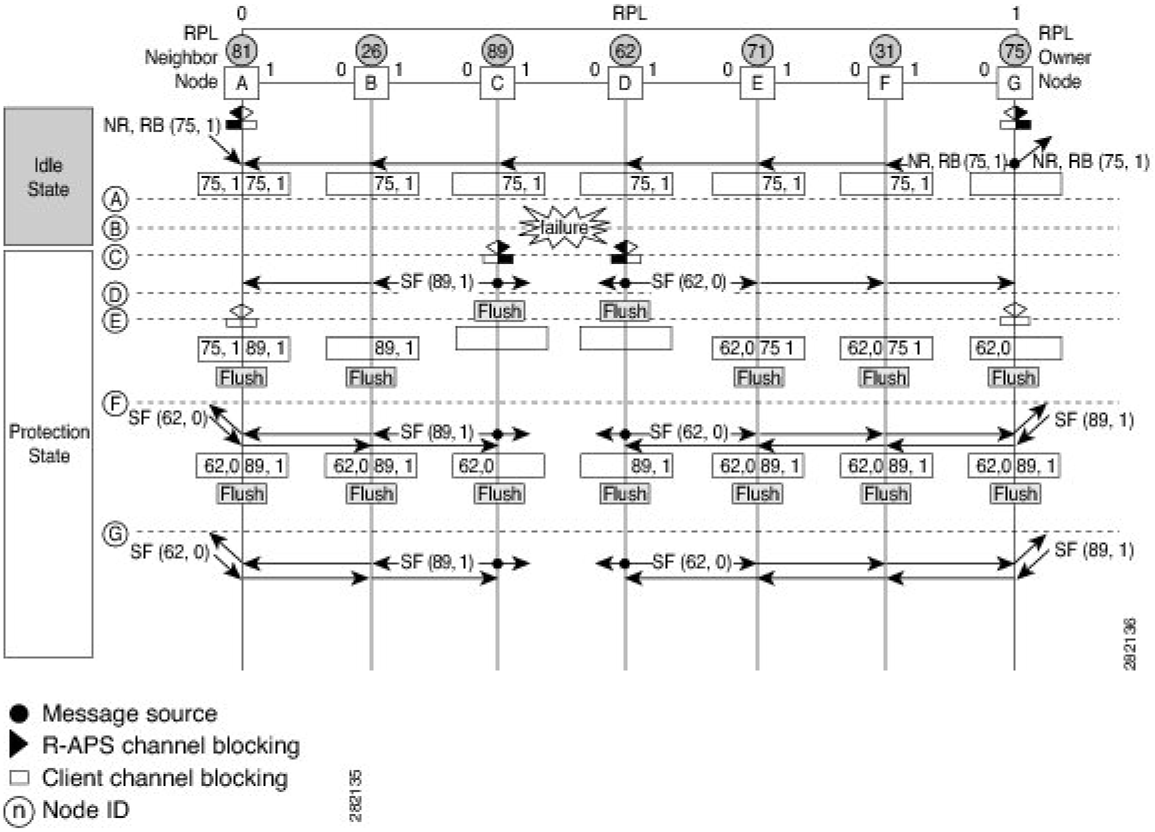
Note The WTB timer interval may be shorter than the WTR timer interval.

- Guard timer—Used by all nodes when changing state; the guard timer blocks latent outdated messages from causing unnecessary state changes. The guard timer can be configured. The default time interval is 500 ms; the time interval ranges from 10 to 2000 ms.
- The recommended Guard Timer for Cisco RSP2 and RSP3 routers is 500 ms.
- Hold-off timers—Used by the underlying Ethernet layer to filter out intermittent link faults. The hold-off timer can be configured. The default time interval is 0 seconds; the time interval ranges from 0 to 10 seconds. Faults are reported to the ring protection mechanism only if this timer expires.

Protection Switching Functionality in a Single Link Failure and Recovery

The following figure illustrates protection switching functionality in a single-link failure.

Figure 7: G.8032 Ethernet Ring Protection Switching in a Single-Link Failure



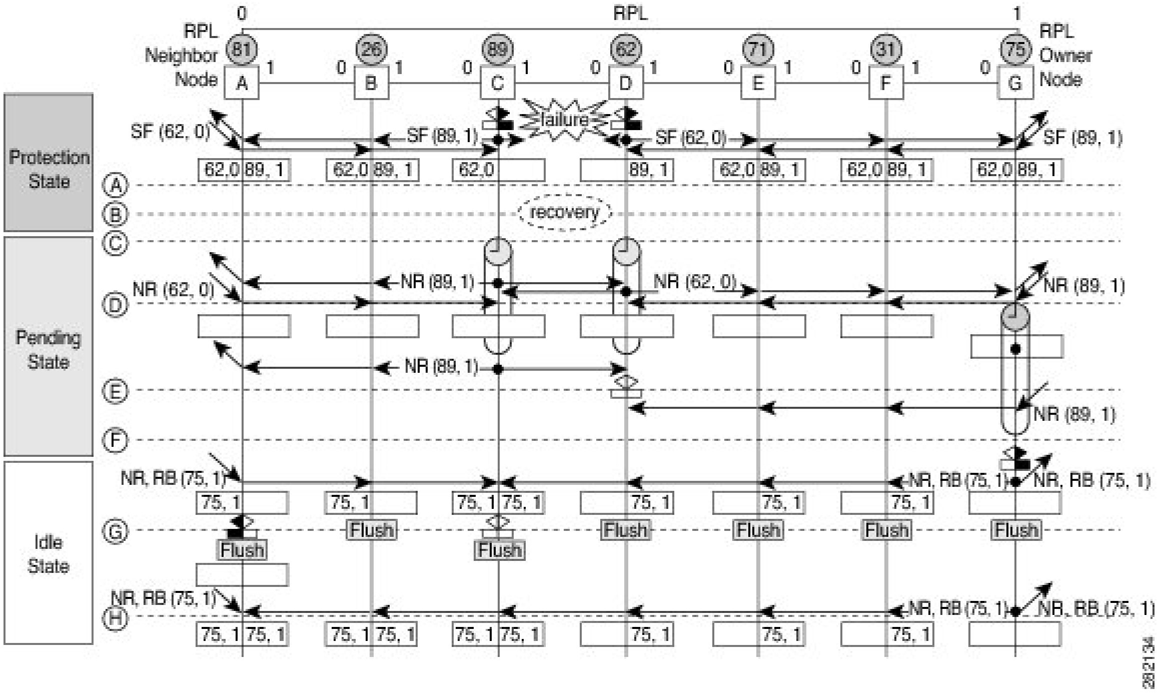
The figure represents an Ethernet ring topology consisting of seven Ethernet ring nodes. The ring protection link (RPL) is the ring link between Ethernet ring nodes A and G. In this topology, both ends of the RPL are blocked. Ethernet ring node G is the RPL owner node, and Ethernet ring node A is the RPL neighbor node.

The following sequence describes the steps followed in the single-link failure:

1. A link operates in the normal condition.
2. A failure occurs.
3. Ethernet ring nodes C and D detect a local signal failure (SF) condition and after the hold-off time interval, block the failed ring port and perform the FDB flush.
4. Ethernet ring nodes C and D start sending Ring Automatic Protection Switching (R-APS) SF messages periodically along with the (node ID and bidirectional path-protected ring (BPR) identifier pair) on both ring ports while the SF condition persists.
5. All Ethernet ring nodes receiving an R-APS SF message perform the FDB flush. When the RPL owner node G and RPL neighbor node A receive an R-APS SF message, the Ethernet ring node unblocks its end of the RPL and performs the FDB flush.
6. All Ethernet ring nodes receiving a second R-APS SF message perform the FDB flush again; the additional FDB flush is because of the node ID and BPR-based configuration.
7. R-APS SF messages are detected on the Ethernet Ring indicating a stable SF condition. Further R-APS SF messages trigger no further action.

The following figure illustrates the steps taken in a revertive operation in a single-link failure.

Figure 8: Single-Link Failure Recovery (Revertive Operation)



The following sequence describes the steps followed in the single-link failure revertive (recovery) operation:

1. A link operates in the stable SF condition.
2. Recovery of link failure occurs.
3. Ethernet ring nodes C and D detect clearing of the SF condition, start the guard timer, and initiate periodic transmission of the R-APS No Request (NR) messages on both ring ports. (The guard timer prevents the reception of R-APS messages.)
4. When the Ethernet ring nodes receive an R-APS NR message, the node ID and BPR identifier pair of a receiving ring port is deleted and the RPL owner node starts the Wait-to-Restore (WTR) timer.
5. When the guard timer expires on Ethernet ring nodes C and D, the nodes may accept the new R-APS messages, if any. Ethernet ring node D receives an R-APS NR message with a higher node ID from Ethernet ring node C, and unblocks its nonfailed ring port.
6. When the WTR timer expires, the RPL owner node blocks its end of the RPL, sends R-APS (NR or route blocked [RB]) message with the (node ID and BPR identifier pair), and performs the FDB flush.
7. When Ethernet ring node C receives an R-APS (NR or RB) message, the node removes the block on its blocked ring ports, and stops sending R-APS NR messages. On the other hand, when the RPL neighbor node A receives an R-APS NR or RB message, the node blocks its end of the RPL. In addition, Ethernet ring nodes A to F perform the FDB flush when receiving an RAPS NR or RB message because of the node ID and BPR-based configuration.

Restrictions for Configuring ITU-T G.8032 Ethernet Ring Protection Switching

- G.8032 does not support more than two ERP instances per ring.
- Admin shut down is highly recommended before making any changes in Connectivity Fault Management (CFM) configuration.
- The **efd notify** command must be used under CFM configuration to notify G.8032 of failures, if any.
- G.8032 support is claimed only over the normal interfaces and not on the port-channels.
- G.8032 is supported only on TEFP.
- Traffic flowing on the G.8032 interface will not be impacted if TERP is manually opened or shut.
- Only 1000 VLANs are supported under TEFP.

How to Configure ITU-T G.8032 Ethernet Ring Protection Switching

Configuring the Ethernet Ring Profile

To configure the Ethernet ring profile, complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet ring g8032 profile** *profile-name*
4. **timer** {**guard** *seconds* | **hold-off** *seconds* | **wtr** *minutes*}
5. **non-revertive**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**ethernet ring g8032 profile** *profile-name* **Example:** `Device(config)# ethernet ring g8032 profile profile1`	Creates the Ethernet ring profile and enters Ethernet ring profile configuration mode.

Step 4	**timer** {**guard** *seconds* | **hold-off** *seconds* | **wtr** *minutes*}
	Example:
	`Device(config-erp-profile)# timer hold-off 5`
		Specifies the time interval for the guard, hold-off, and Wait-to-Restore (WTR) timers.

Step 5	**non-revertive** **Example:** `Device(config-erp-profile)# non-revertive`	Specifies a nonrevertive Ethernet ring instance. • By default, Ethernet ring instances are revertive.

Step 6	**end**
	Example:
	`Device(config-erp-profile)# end`
		Returns to user EXEC mode.

Configuring Ethernet CFM MEPs

Configuring Ethernet Connectivity Fault Management (CFM) maintenance endpoints (MEPs) is optional although recommended for fast failure detection and CFM monitoring. When CFM monitoring is configured, note the following points:

- Static remote MEP (RMEP) checking should be enabled.
- The MEPs should be configured to enable Ethernet fault detection.

For information about configuring Ethernet Connectivity Fault Management (CFM) maintenance endpoints (MEPs), see the “Configuring Ethernet Connectivity Fault Management in a Service Provider Network” module of the *Carrier Ethernet Configuration Guide*.

Enabling Ethernet Fault Detection for a Service

To enable Ethernet Fault Detection (EFD) for a service to achieve fast convergence, complete the following steps

Note Link protection is not supported on the RSP3 Module.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm global**
4. **ethernet cfm domain**_domain-name_ **level** _level-id_ [**direction outward**]
5. **service** {_ma-name_ | _ma-num_ | **vlan-id** _vlan-id_ | **vpn-id** _vpn-id_} [**port** | **vlan** _vlan-id_ [**direction down**]]
6. **continuity-check** [**interval** _time_ | **loss-threshold** _threshold_ | **static rmep**]
7. **efd notify g8032**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ethernet cfm global** **Example:** `Device(config)# ethernet cfm global`	Enables Ethernet CFM globally.
Step 4	**ethernet cfm domain**_domain-name_ **level** _level-id_ [**direction outward**] **Example:** `Device(config)# ethernet cfm domain G8032 level 4`	Configures the CFM domain for ODU 1 and enters Ethernet CFM configuration mode.

Step 5	**service** {_ma-name_	_ma-num_	**vlan-id** _vlan-id_	**vpn-id** _vpn-id_} [**port**	**vlan** _vlan-id_ [**direction down**]]
					Example:
					`Device(config-ecfm)# service 8032_service evc`
					`8032-evc vlan 1001 direction down`
						Defines a maintenance association for ODU 1 and enters Ethernet CFM service instance configuration mode.

Step 6	**continuity-check** [**interval** _time_	**loss-threshold** _threshold_	**static rmep**]
			Example:
			`Device(config-ecfm-srv)# continuity-check interval`
			` 3.3ms`
				Enables the transmission of continuity check messages (CCMs).

	Command or Action	Purpose
Step 7	**efd notify g8032** **Example:** `Device(config-ecfm-srv)# efd notify g8032`	Enables CFM to notify registered protocols when a defect is detected or cleared, which matches the current fault alarm priority.

Step 8	**end**
	Example:
	`Device(config-ecfm-srv)# end`
		Returns to user EXEC mode.

Configuring the Ethernet Protection Ring

To configure the Ethernet Protection Ring (EPR), complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet ring g8032** *ring-name*
4. **port0 interface** *type number*
5. **monitor service instance** *instance-id*
6. **exit**
7. **port1** {**interface***type number* | **none**}
8. **monitor service instance** *instance-id*
9. **exit**
10. **exclusion-list vlan-ids** *vlan-id*
11. **open-ring**
12. **instance** *instance-id*
13. **description** *descriptive-name*
14. **profile** *profile-name*
15. **rpl** {**port0** | **port1**} {**owner** | **neighbor** | **next-neighbor** }
16. **inclusion-list vlan-ids** *vlan-id*
17. **aps-channel**
18. **level** *level-value*
19. **port0 service instance** *instance-id*
20. **port1 service instance** {*instance-id* | **none** }
21. **end**

DETAILED STEPS

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

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ethernet ring g8032** *ring-name* **Example:** `Device(config)# ethernet ring g8032 ring1`	Specifies the Ethernet ring and enters Ethernet ring port configuration mode.
Step 4	**port0 interface** *type number* **Example:** `Device(config-erp-ring)# port0 interface gigabitethernet 0/1/0`	Connects port0 of the local node of the interface to the Ethernet ring and enters Ethernet ring protection mode.
Step 5	**monitor service instance** *instance-id* **Example:** `Device(config-erp-ring-port)# monitor service instance 1`	Assigns the Ethernet service instance to monitor the ring port (port0) and detect ring failures.
Step 6	**exit** **Example:** `Device(config-erp-ring-port)# exit`	Exits Ethernet ring port configuration mode.

Step 7	**port1** {**interface***type* *number* | **none**}
	Example:
	`Device(config-erp-ring)# port1 interface gigabitethernet 0/1/1`
		Connects port1 of the local node of the interface to the Ethernet ring and enters Ethernet ring protection mode.

Step 8	**monitor service instance** *instance-id* **Example:** `Device(config-erp-ring-port)# monitor service instance 2`	Assigns the Ethernet service instance to monitor the ring port (port1) and detect ring failures. • The interface (to which port1 is attached) must be a subinterface of the main interface.
Step 9	**exit** **Example:** `Device(config-erp-ring-port)# exit`	Exits Ethernet ring port configuration mode.
Step 10	**exclusion-list vlan-ids** *vlan-id* **Example:**	Specifies VLANs that are unprotected by the Ethernet ring protection mechanism.

	Command or Action	Purpose
	`Device(config-erp-ring)# exclusion-list vlan-ids 2`	
Step 11	**open-ring** **Example:** `Device(config-erp-ring)# open-ring`	Specifies the Ethernet ring as an open ring.
Step 12	**instance** *instance-id* **Example:** `Device(config-erp-ring)# instance 1`	Configures the Ethernet ring instance and enters Ethernet ring instance configuration mode.
Step 13	**description** *descriptive-name* **Example:** `Device(config-erp-inst)# description cisco_customer_instance`	Specifies a descriptive name for the Ethernet ring instance.
Step 14	**profile** *profile-name* **Example:** `Device(config-erp-inst)# profile profile1`	Specifies the profile associated with the Ethernet ring instance.

Step 15	**rpl** {**port0** | **port1**} {**owner** | **neighbor** | **next-neighbor** }
	Example:
	`Device(config-erp-inst)# rpl port0 neighbor`
		Specifies the Ethernet ring port on the local node as the RPL owner, neighbor, or next neighbor.

Step 16	**inclusion-list vlan-ids** *vlan-id* **Example:** `Device(config-erp-inst)# inclusion-list vlan-ids 11`	Specifies VLANs that are protected by the Ethernet ring protection mechanism. **Note** VLANs should be within or equal to VLAN configured in the interface.
Step 17	**aps-channel** **Example:** `Device(config-erp-inst)# aps-channel`	Enters Ethernet ring instance aps-channel configuration mode.
Step 18	**level** *level-value* **Example:** `Device(config-erp-inst-aps)# level 5`	Specifies the Automatic Protection Switching (APS) message level for the node on the Ethernet ring. • All nodes in the Ethernet ring must be configured with the same level.

	Command or Action	Purpose
Step 19	**port0 service instance** *instance-id* **Example:** `Device(config-erp-inst-aps)# port0 service instance 100`	Associates APS channel information with port0.

Step 20	**port1 service instance** {*instance-id* **| none** }
	Example:
	`Device(config-erp-inst-aps)# port1 service instance 100`
		Associates APS channel information with port1.

Step 21	**end**
	Example:
	`Device(config-erp-inst-aps)# end`
		Returns to user EXEC mode.

Configuring Topology Change Notification Propagation

To configure topology change notification (TCN) propagation, complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet tcn-propagation G8032 to {REP | G8032}**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	**ethernet tcn-propagation G8032 to {REP | G8032}**
	Example:
	`Device(config)# ethernet tcn-propagation G8032 to G8032`
		Allows topology change notification (TCN) propagation from a source protocol to a destination protocol.
		• Source and destination protocols vary by platform and release.

	Command or Action	Purpose

Step 4	**end**
	Example:
	`Device(config)# end`
		Returns to user EXEC mode.

Configuring TEFP

To configure a service instance, complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **service instance trunk** *instance-id* **ethernet**
5. **encapsulation dot1q** *range of vlan-id*
6. **bridge-domain from-encapsulation**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/0`	Specifies the interface type and number.
Step 4	**service instance trunk** *instance-id* **ethernet** **Example:** `Device(config-if)# service instance trunk 101 ethernet`	Creates a service instance on an interface and enters service instance configuration mode.

	Command or Action	Purpose
Step 5	**encapsulation dot1q** *range of vlan-id* **Example:** `Device(config-if-srv)# encapsulation dot1q 13`	Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.
Step 6	**bridge-domain from-encapsulation** **Example:** `Device(config-if-srv)# bridge-domain from-encapsulation`	Binds the service instance to a bridge domain instance.

Step 7	**end**
	Example:
	`Device(config-if-srv)# end`
		Exits service instance configuration mode.

Verifying the Ethernet Ring Protection (ERP) Switching Configuration

To verify the ERP switching configuration, use one or more of the following commands in any order.

Note Follow these rules while adding or deleting VLANs from the inclusion list:

- While adding VLAN into the inclusion list, it has to be first added on the interface and then in the G.8032 inclusion list.
- While removing VLAN from the inclusion list, it has to be removed from the G.8032 inclusion list and then from the interface.

Addition or Deletion of VLANs in exclusion list is not supported.

SUMMARY STEPS

1. **enable**
2. **show ethernet ring g8032 status** [*ring-name*] [**instance** [*instance-id*]]
3. **show ethernet ring g8032 brief** [*ring-name*] [**instance** [*instance-id*]]
4. **show ethernet ring g8032 summary**
5. **show ethernet ring g8032 statistics** [*ring-name*] [**instance** [*instance-id*]]
6. **show ethernet ring g8032 profile** [*profile-name*]
7. **show ethernet ring g8032 port status interface** [*type number*]
8. **show ethernet ring g8032 configuration** [*ring-name*] **instance** [*instance-id*]
9. **show ethernet ring g8032 trace** {**ctrl** [*ring-name* **instance** *instance-id*] | **sm**}
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ethernet ring g8032 status** [*ring-name*] [**instance** [*instance-id*]] **Example:** `Device# show ethernet ring g8032 status RingA instance 1`	Displays a status summary for the ERP instance.
Step 3	**show ethernet ring g8032 brief** [*ring-name*] [**instance** [*instance-id*]] **Example:** `Device# show ethernet ring g8032 brief`	Displays a brief description of the functional state of the ERP instance.
Step 4	**show ethernet ring g8032 summary** **Example:** `Device# show ethernet ring g8032 summary`	Displays a summary of the number of ERP instances in each state of the ERP switching process.
Step 5	**show ethernet ring g8032 statistics** [*ring-name*] [**instance** [*instance-id*]] **Example:** `Device# show ethernet ring g8032 statistics RingA instance 1`	Displays the number of events and Ring Automatic Protection Switching (R-APS) messages received for an ERP instance.
Step 6	**show ethernet ring g8032 profile** [*profile-name*] **Example:** `Device# show ethernet ring g8032 profile gold`	Displays the settings for one or more ERP profiles.
Step 7	**show ethernet ring g8032 port status interface** [*type number*] **Example:** `Device# show ethernet ring g8032 port status interface  gigabitethernet 0/0/1`	Displays Ethernet ring port status information for the interface.
Step 8	**show ethernet ring g8032 configuration** [*ring-name*] **instance** [*instance-id*] **Example:**	Displays the details of the ERP instance configuration manager.

	Command or Action	Purpose
	`Device# show ethernet ring g8032 configuration RingA instance 1`	
Step 9	**show ethernet ring g8032 trace** {**ctrl** [*ring-name* **instance** *instance-id*] | **sm**} **Example:** `Device# show ethernet ring g8032 trace sm`	Displays information about ERP traces.

Step 10	**end**
	Example:
	`Device# end`
		Returns to privileged EXEC mode.

Configuration Examples for ITU-T G.8032 Ethernet Ring Protection Switching

Example: Configuring Ethernet Ring Protection Switching

The following is an example of an Ethernet Ring Protection (ERP) switching configuration:

```
ethernet ring g8032 profile profile_ABC
 timer wtr 1
 timer guard 100
 timer hold-off  1

ethernet ring g8032 major_ring_ABC
 exclusion-list vlan-ids 1000
 port0 interface GigabitEthernet 0/0/0
  monitor service instance 103
 port1 interface GigabitEthernet 0/0/1
  monitor service instance 102
 instance 1
  profile profile_ABC
  rpl port0 owner
  inclusion-list vlan-ids 100
  aps-channel
   port0 service instance 100
   port1 service instance 100
  !
GigabitEthernet0/0/0
mtu 9216
 no ip address
 negotiation auto
 service instance trunk 1 ethernet
  encapsulation dot1q 60-61
  rewrite ingress tag pop 1 symmetric
  bridge-domain from-encapsulation

 !
```

```
!
```

Example: Enabling Ethernet Fault Detection for a Service

```
ethernet cfm domain G8032 level 4
service 8032_service evc 8032-evc vlan 1001 direction down
  continuity-check
  continuity-check interval 3.3ms
   efd notify g8032
ethernet ring g8032 profile TEST
timer wtr 1
timer guard 100
ethernet ring g8032 open
open-ring
port0 interface GigabitEthernet0/0/0
  monitor service instance 1001
port1 none
instance 1
  profile TEST
  inclusion-list vlan-ids 2-500,1001
  aps-channel
   port0 service instance 1001
   port1 none
  !
!
instance 2
  profile TEST
  rpl port0 owner
  inclusion-list vlan-ids 1002,1005-2005
  aps-channel
   port0 service instance 1002
   port1 none
  !

interface GigabitEthernet0/0/0
no ip address
load-interval 30
shutdown
negotiation auto
storm-control broadcast level 10.00
storm-control multicast level 10.00
storm-control unicast level 90.00
service instance 1 ethernet
  encapsulation untagged
  l2protocol peer lldp
  bridge-domain 1
!
service instance trunk 10 ethernet
  encapsulation dot1q 2-500,1005-2005
  rewrite ingress tag pop 1 symmetric
  bridge-domain from-encapsulation
!
service instance 1001 ethernet 8032-evc
  encapsulation dot1q 1001
  rewrite ingress tag pop 1 symmetric
  bridge-domain 1001
  cfm mep domain G8032 mpid 20
!
service instance 1002 ethernet 8032-evc-1
  encapsulation dot1q 1002
  rewrite ingress tag pop 1 symmetric
  bridge-domain 1002
!
End
```

Example: Verifying the Ethernet Ring Protection Configuration

The following is sample output from the **show ethernet ring g8032 configuration** command. Use this command to verify if the configuration entered is valid and to check for any missing configuration parameters.

```
Device# show ethernet ring g8032 configuration

ethernet ring ring0
 Port0: GigabitEthernet0/0/0 (Monitor: GigabitEthernet0/0/0)
 Port1: GigabitEthernet0/0/4 (Monitor: GigabitEthernet0/0/4)
 Exclusion-list VLAN IDs: 4001-4050
 Open-ring: no
 Instance 1
  Description:
  Profile:     opp
  RPL:
  Inclusion-list VLAN IDs: 2,10-500
  APS channel
   Level: 7
   Port0: Service Instance 1
   Port1: Service Instance 1
  State: configuration resolved
```

CHAPTER 5

Multiple Spanning Tree Protocol

The Multiple Spanning Tree Protocol (MSTP) is an STP variant that allows multiple and independent spanning trees to be created over the same physical network. The parameters for each spanning tree can be configured separately, so as to cause a different network devices to be selected as the root bridge or different paths to be selected to form the loop-free topology. Consequently, a given physical interface can be blocked for some of the spanning trees and unblocked for others.

Having set up multiple spanning trees, the set of VLANs in use can be partitioned among them; for example, VLANs 1 - 100 can be assigned to spanning tree 1, VLANs 101 - 200 can be assigned to spanning tree 2, VLANs 201 - 300 can be assigned to spanning tree 3, and so on. Since each spanning tree has a different active topology with different active links, this has the effect of dividing the data traffic among the available redundant links based on the VLAN - a form of load balancing.

Restrictions for configuring MSTP

- RSTP is not supported. To support RSTP, all vlans are mapped to MSTI 0 when no instance is created for MSTP.
- PVSTP is *not* supported.
- Supports only 16 instances.
- Untagged EVCs do not participate in MST loop detection.

How to Configure MST Protocol

This section describes the procedure for configuring MSTP:

Enabling Multiple Spanning Tree Protocol

By default, MSTP is disabled on all interfaces. MSTP need not be enabled explicitly on each interfaces. By turning the global configuration on, it is enabled on all interfaces.

Configuring Multiple Spanning Tree Protocol

Describes steps to configure MST

SUMMARY STEPS

1. **configure**
2. **spanning-tree mode mst**
3. **spanning-tree mst configuration**
4. **instance** *vlan-id* **vlan** *vlan-range*
5. **name** *region*
6. **revision** *revision -number*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure** **Example:** `Device> configure`	Enters global configuration mode.
Step 2	**spanning-tree mode mst** **Example:** `Device> spanning-tree mode mst`	Enables MSTP configuration mode.
Step 3	**spanning-tree mst configuration** **Example:** `Device(config)#spanning-tree mst configuration`	Enters the MSTP configuration submode.
Step 4	**instance** *vlan-id* **vlan** *vlan-range* **Example:** `Device(config-mstp-inst)# instance 1 vlan 450-480`	Maps the VLANs to an MST instance
Step 5	**name** *region* **Example:** `Device(config-mstp)# name m1`	Sets the name of the MSTP region.
Step 6	**revision** *revision -number* **Example:** `Device(config-mstp)#)revision 1`	Sets the revision level of the MSTP region.

Step 7	**end**
	Example:
	`Device(config-mstp-if)# end`
		Returns to privileged EXEC mode.

Configuring Untagged EFP over MST Interface

Describes steps to configure untagged EFP over MST:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface number*
4. **no ip address**
5. **service instance** *number* **ethernet** *[name]*
6. **bridge-domain** *bridge-id*
7. **encapsulation untagged**
8. **l2protocol peer stp**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface number* **Example:** `Router(config)# interface gigabitEthernet 0/0/5`	Specifies the Gigabit Ethernet interface to configure, where: slot/subslot/port-Specifies the location of the interface.
Step 4	**no ip address** **Example:** `Router (config-if)# no ip address`	Disables the IP address on the interface.
Step 5	**service instance** *number* **ethernet** *[name]* **Example:** `Router (config-if)#service instance 200 ethernet`	Configure an EFP (service instance) and enter service instance configuration mode.
Step 6	**bridge-domain** *bridge-id* **Example:** `Router (config-if-srv)#  bridge-domain from-encapsulation`	Creates a list of bridge domains for an EFP trunk port using the bridge-domain IDs derived from the encapsulation VLAN numbers.
Step 7	**encapsulation untagged** **Example:** `Router (config-if-srv)# encapsulation untagged`	Configures the encapsulation. Defines the matching criteria that maps the untagged frames on an interface for the appropriate service instance.

	Command or Action	Purpose
Step 8	**l2protocol peer stp** **Example:** `Router (config-if-srv)# l2protocol peer stp`	Configures STP to peer with a neighbor on a port that has an EFP service instance.

Step 9	**end**
	Example:
	`Device(config-mstp-if)# end`
		Returns to privileged EXEC mode.

Configuration Example

This example shows how to configure STP to peer with a neighbor on a service instance.

```
interface GigabitEthernet0/0/0
no ip address
negotiation auto
service instance trunk 10 ethernet
  encapsulation dot1q 10-20
  bridge-domain from-encapsulation
!
service instance 1024 ethernet
  encapsulation untagged
  l2protocol peer stp
  bridge-domain 1024
!
end
```

CHAPTER 6

Configuring Flex Links

This chapter describes how to configure Flex Links, a pair of Layer 2 interfaces, where one interface is configured to act as a backup to the other.

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Configuring Flex Links

- You can configure only one Flex Link backup link for any active link, and it must be a different interface from the active interface.
- An interface can belong to only one Flex Link pair. An interface can be a backup link for only one active link. An active link cannot belong to another Flex Link pair.
- Neither of the links can be a port that belongs to an EtherChannel nor port channel
- A backup link does not have to be the same type (TenGigabit Ethernet, Gigabit Ethernet) as the active link.
- STP is disabled on Flex Link ports. If STP is configured on the switch, Flex Links do not participate in STP in all VLANs in which STP is configured. With STP not running, be sure that there are no loops in the configured topology.
- Flex link is only supported on trunk EFP.

- In bi-directional traffic, FlexLink Convergence will be high in one-direction due to mac address black holing.
- Admin shut has no effect on interfaces that are configured under flexlinks.
- Dynamically editing encapsulations using *add* and *remove* options is not supported.
- Dynamic editting or overwriting VLANs on Active and Backup causes traffic loop.

Note Remove **ethernet backup** command from primary flexlink interface and then edit the VLANs of primary and backup interfaces.

Information About Flex Links

The feature provides an alternative solution to the Spanning Tree Protocol (STP), allowing you to turn off STP and still provide basic link redundancy. Flex Links are typically configured in service provider or enterprise networks, where, you do not want to run STP on the router. If the router is running STP, it is not necessary to configure Flex Links, because STP already provides link-level redundancy or backup. Flex Links are supported only on Trunk EFP and are not supported on other EVCs.

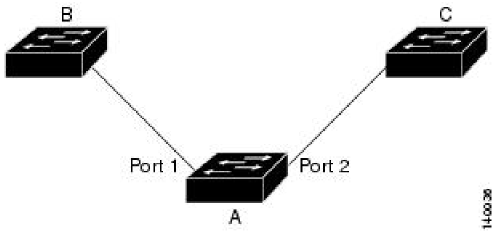
Following are the two flex link modes supported:

- Active-Alone Forwarding Method
- Active-Backup-Both Forwarding Method

Active-Alone forwarding Method

From the schematic representation, ports 1 and 2 on switch A are connected to uplink switches B and C. Because they are configured as Flex Links Active-Alone forwarding mode, only one of the interfaces forwards traffic; the other is in standby mode. If port 1 is the active link, it begins forwarding traffic between port 1 and switch B; the link between port 2 (the backup link) and switch C do not forward traffic. If port 1 goes down, port 2 comes up and starts forwarding traffic to switch C. Since pre-emption is not supported, even after port 1 comes back to operational state, traffic continues to be forwarded to port 2. Switch over back to port 1 happens only when port 2 goes down.

Figure 9: Active-Alone Forwarding Method



Configuring Active Alone Forwarding Method

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **no shutdown**
5. **ethernet backup interface** *interface-id*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Router(config)# interface gigabitEthernet 0/0/5`	Specify the interface, and enter interface configuration mode. The interface can be a physical Layer 2 interface.
Step 4	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enable the port, if necessary. By default, UNIs are disabled, and NNIs are enabled.
Step 5	**ethernet backup interface** *interface-id* **Example:** `Router(config)# ethernet backup interface gigabitEthernet 0/0/5`	Configure a physical Layer 2 interface as part of a Flex Link pair with the interface. When one link is forwarding traffic, the other interface is in standby mode.

Step 6	**end**
	Example:
	`Router(config-if)# end`
		Return to privileged EXEC mode.

Configuration Example

```
On Active interface(Port 5)

Router> enable
Router# configure terminal
Router# service instance trunk 1000 ethernet
Router# encapsulation dot1q 1-1000
```

```
Router# rewrite ingress tag pop 1 symmetric
Router# bridge-domain from-encapsulation



Backup interface (Port 6)

Router> enable
Router# configure terminal
Router# service instance trunk 1000 ethernet
Router# encapsulation dot1q 1-1000
Router# rewrite ingress tag pop 1 symmetric
Router# bridge-domain from-encapsulation



Flexlink Configuration

Router> enable
Router# configure terminal
Router(config)# interface gigabitEthernet 0/0/5
Router(config-if)# no shutdown
Router(config-if)# ethernet backup interface gigabitEthernet 0/0/6
Router(config-if)# end
```

Verifying Active Alone Forwarding Method Configuration

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **show ethernet backup detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**show ethernet backup detail** **Example:** `Router# show ethernet backup detail`	This displays the flex link configuration.

Configuration Output

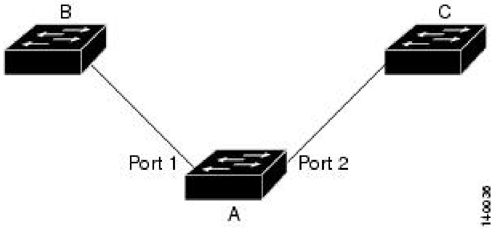
```
Switch Backup Interface Pairs:
```

```
Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet0/0/5    Te0/0/12                Active Up/Backup Standby
        Preemption Mode  : off
        Multicast Fast Convergence  : Off
        Bandwidth : 1000000 Kbit (Gi0/0/3), 1000000 Kbit (Te0/0/12)
        Mac Address Move Update Vlan : auto
        Forwarding  : Active-Only
```

Active-Backup-Both forwarding Method

From the schematic representation, ports 1 and 2 on switch A are connected to uplink switches B and C. Because they are configured as Flex Link in active-backup both forwarding mode, both the interfaces will be forwarding traffic. If port 1 is the active link, all mutually inclusive vlans (common vlans configured in both active / backup interface) would be forwarded on active interface and mutually exclusive vlans would be forwarded from the respective active / backup interfaces. If port 1 goes down, then port 2 will start forwarding only the traffic for the common vlans along with its specific exclusive vlans. All traffic belonging to the exclusive vlans as part of active interface configuration would be dropped until port 1 comes back to operational state.

Figure 10: Active-Backup-Both Forwarding Method



Configuring Active Backup Both Forwarding Method

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **no shutdown**
5. **ethernet backup interface** *interface-id* **prefer forwarding**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**interface** *interface-id* **Example:** `Router(config)# interface gigabitEthernet 0/0/8`	Specify the interface, and enter interface configuration mode. The interface can be a physical Layer 2 interface .
Step 4	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enable the port, if necessary. By default, UNIs are disabled, and NNIs are enabled.
Step 5	**ethernet backup interface** *interface-id* **prefer forwarding** **Example:** `Router(config)# ethernet backup interface gigabitEthernet 0/0/8 prefer forwarding`	Configure a physical Layer 2 interface as part of a Flex Link pair with the interface. When one link is forwarding traffic, the other interface is in standby mode.

Step 6	**end**
	Example:
	`Router(config-if)# end`
		Return to privileged EXEC mode.

Configuration Example

```
On Active interface(Port 7)

Router> enable
Router# configure terminal
Router# service instance trunk 1000 ethernet
Router# encapsulation dot1q 1-512
Router# rewrite ingress tag pop 1 symmetric
Router# bridge-domain from-encapsulation



Backup interface (Port 8)

Router> enable
Router# configure terminal
Router# service instance trunk 1000 ethernet
Router# encapsulation dot1q 512-1000
Router# rewrite ingress tag pop 1 symmetric
Router# bridge-domain from-encapsulation



Flexlink Configuration

Router> enable
Router# configure terminal
Router(config)# interface gigabitEthernet 0/0/7
Router(config-if)# no shutdown

Router(config-if)# ethernet backup interface gigabitEthernet 0/0/7 prefer forwarding
Router(config-if)# end
```

Verifying Active-Backup-Both Forwarding Method Configuration

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **show ethernet backup detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**show ethernet backup detail** **Example:** `Router# show ethernet backup detail`	This displays the flex link configuration.

Configuration Output

```
Switch Backup Interface Pairs:
Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet0/0/3    Te0/0/12                Active Up/Backup Standby
        Preemption Mode  : off
        Multicast Fast Convergence  : Off
        Bandwidth : 1000000 Kbit (Gi0/0/3), 1000000 Kbit (Te0/0/12)
        Mac Address Move Update Vlan : auto
        Forwarding  : Active-Backup-Both
```

Unsupported Functions

Following functions are not supported:

- MMU Notification
- IGMP Fast convergence
- Preemption Support
- Flex links support on a Port channel interface.
- Flex links support on EVC

- Flex links with VLB
- Flex links on IP configured Physical interface.
- Flexlink cannot be configured on a REP / G8032 configured interface and vice-versa.
- STP can be enabled globally but will not be applied on flex link configured interfaces alone.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html

Standards and RFCs

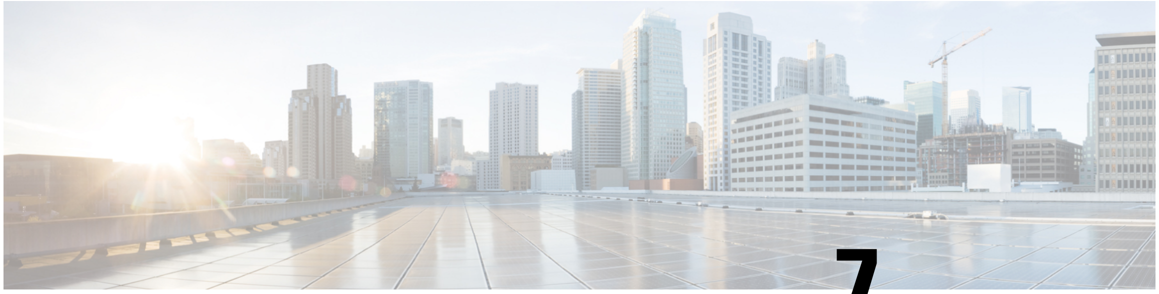
Standard/RFC	Title
No specific Standards and RFCs are supported by the features in this document.	—

MIBs

MIB	MIBs Link
—	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

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.	http://www.cisco.com/cisco/web/support/index.html



CHAPTER 7

Configuring PVST+ and RPVST+

This chapter describes how to configure the Spanning Tree Protocol (STP) on port-based VLANs on the Cisco router. The router can use the per-VLAN spanning-tree plus (PVST+) protocol based on the IEEE 802.1D standard and Cisco proprietary extensions, or the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol based on the IEEE 802.1w standard.

For information about the Multiple Spanning Tree Protocol (MSTP) and how to map multiple VLANs to the same spanning-tree instance, see the Multiple Spanning Tree Protocol chapter.

Note For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

STP Overview

STP is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages. Switches might also learn end-station MAC addresses on multiple Layer 2 interfaces. These conditions result in an unstable network. Spanning-tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

The STP uses a spanning-tree algorithm to select one switch of a redundantly connected network as the root of the spanning tree. The algorithm calculates the best loop-free path through a switched Layer 2 network by assigning a role to each port based on the role of the port in the active topology:

- Root—A forwarding port elected for the spanning-tree topology
- Designated—A forwarding port elected for every switched LAN segment
- Alternate—A blocked port providing an alternate path to the root bridge in the spanning tree
- Backup—A blocked port in a loopback configuration

The switch that has *all* of its ports as the designated role or the backup role is the root switch. The switch that has at least *one* of its ports in the designated role is called the designated switch.

Spanning tree forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning-tree algorithm recalculates the spanning-tree topology and activates the standby path. Switches send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals. The switches do not forward these frames but use them to construct a loop-free path. BPDUs contain information about the sending switch and its ports, including switch and MAC addresses, switch priority, port priority, and path cost. Spanning tree uses this information to elect the root switch and root port for the switched network and the root port and designated port for each switched segment.

When two ports on a switch are part of a loop, the spanning-tree port priority and path cost settings control which port is put in the forwarding state and which is put in the blocking state. The spanning-tree port priority value represents the location of a port in the network topology and how well it is located to pass traffic. The path cost value represents the media speed.

Spanning-Tree Topology and BPDUs

The stable, active spanning-tree topology of a switched network is controlled by these elements:

- The unique bridge ID (switch priority and MAC address) associated with each VLAN on each switch.
- The spanning-tree path cost to the root switch.
- The port identifier (port priority and MAC address) associated with each Layer 2 STP-enabled interface.

When the switches in a network are powered up, each functions as the root switch. Each switch sends a configuration BPDU through all of its ports only through the STP-enabled ports. The BPDUs communicate and compute the spanning-tree topology. Each configuration BPDU contains this information:

- The unique bridge ID of the switch that the sending switch identifies as the root switch
- The spanning-tree path cost to the root
- The bridge ID of the sending switch
- Message age

- The identifier of the sending interface
- Values for the hello, forward delay, and max-age protocol timers

When a switch receives a configuration BPDU that contains *superior* information (lower bridge ID, lower path cost, and so forth), it stores the information for that port. If this BPDU is received on the root port of the switch, the switch also forwards it with an updated message to all attached LANs for which it is the designated switch.

If a switch receives a configuration BPDU that contains *inferior* information to that currently stored for that port, it discards the BPDU. If the switch is a designated switch for the LAN from which the inferior BPDU was received, it sends that LAN a BPDU containing the up-to-date information stored for that port. In this way, inferior information is discarded, and superior information is propagated on the network.

A BPDU exchange results in these actions:

- One switch in the network is elected as the root switch (the logical center of the spanning-tree topology in a switched network).

For each VLAN, the switch with the highest switch priority (the lowest numerical priority value) is elected as the root switch. If all switches are configured with the default priority (32768), the switch with the lowest MAC address in the VLAN becomes the root switch. The switch priority value occupies the most significant bits of the bridge ID, as shown in tables Switch Priority Value and Extended System ID and Spanning-Tree Timer.

- A root port is selected for each switch (except the root switch). This port provides the best path (lowest cost) when the switch forwards packets to the root switch.
- The shortest distance to the root switch is calculated for each switch based on the path cost.
- A designated switch for each LAN segment is selected. The designated switch incurs the lowest path cost when forwarding packets from that LAN to the root switch. The port through which the designated switch is attached to the LAN is called the designated port.

All paths that are not needed to reach the root switch from anywhere in the switched network are placed in the spanning-tree blocking mode.

Bridge ID, Switch Priority, and Extended System ID

The IEEE 802.1D standard requires that each switch has an unique bridge identifier (bridge ID), which controls the selection of the root switch. Because each VLAN is considered as a different *logical bridge* with PVST+ and rapid PVST+, the same switch must have as many different bridge IDs as VLANs configured on it. Each VLAN on the switch has a unique 8-byte bridge ID. The two most-significant bytes are used for the switch priority, and the remaining six bytes are derived from the switch MAC address.

The switch supports the IEEE 802.1t spanning-tree extensions, and some of the bits previously used for the switch priority are now used as the VLAN identifier. The result is that fewer MAC addresses are reserved for the switch, and a larger range of VLAN IDs can be supported, all while maintaining the uniqueness of the bridge ID. As shown in table Switch Priority Value and Extended System ID, the two bytes previously used for the switch priority are reallocated into a 4-bit priority value and a 12-bit extended system ID value equal to the VLAN ID.

Table 1: Switch Priority Value and Extended System ID

Switch Priority Value				Extended System ID (Set Equal to the VLAN ID)											
Bit 16	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

Spanning tree uses the extended system ID, the switch priority, and the allocated spanning-tree MAC address to make the bridge ID unique for each VLAN.

Support for the extended system ID affects how you manually configure the root switch, the secondary root switch, and the switch priority of a VLAN. For example, when you change the switch priority value, you change the probability that the switch will be elected as the root switch. Configuring a higher value decreases the probability; a lower value increases the probability. For more information, see the Configuring the Root Switch section, the Configuring a Secondary Root Switch section, and the Configuring the Switch Priority of a VLAN section.

Spanning-Tree Interface States

Propagation delays can occur when protocol information passes through a switched LAN. As a result, topology changes can take place at different times and at different places in a switched network. When an STP port transitions directly from nonparticipation in the spanning-tree topology to the forwarding state, it can create temporary data loops. Interfaces must wait for new topology information to propagate through the switched LAN before starting to forward frames. They must allow the frame lifetime to expire for forwarded frames that have used the old topology.

Each Layer 2 interface on a switch using spanning tree exists in one of these states:

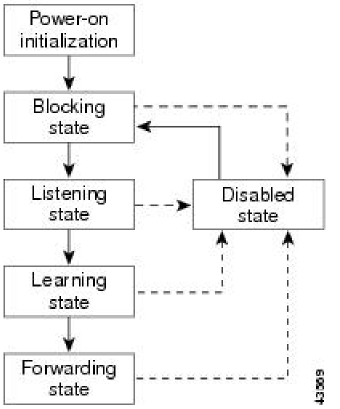
- Blocking—The interface does not participate in frame forwarding.
- Listening—The first transitional state after the blocking state when the spanning tree determines that the interface should participate in frame forwarding.
- Learning—The interface prepares to participate in frame forwarding.
- Forwarding—The interface forwards frames.
- Disabled—The interface is not participating in spanning tree because of a shutdown port, no link on the port, or no spanning-tree instance running on the port.

A port participating in spanning tree moves through these states:

- From initialization to blocking
- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled

The figure below shows how an interface moves through the states.

Figure 11: Spanning-Tree Interface States



Spanning tree is not enabled by default. Once the spanning tree mode is selected, each VLAN on ports goes through the blocking state and the transitionary states of listening and learning. Spanning tree stabilizes each interface at the forwarding or blocking state.

When the spanning-tree algorithm places a Layer 2 spanning-tree interface in the forwarding state, this process occurs:

1. The interface is in the listening state while spanning tree waits for protocol information to transition the interface to the blocking state.
2. While spanning tree waits the forward-delay timer to expire, it moves the interface to the learning state and resets the forward-delay timer.
3. In the learning state, the interface continues to block frame forwarding as the switch learns end-station location information for the forwarding database.
4. When the forward-delay timer expires, spanning tree moves the interface to the forwarding state, where both learning and frame forwarding are enabled.

Blocking State

A Layer 2 interface in the blocking state does not participate in frame forwarding. After initialization, a BPDU is sent to each switch interface, or to each switch STP port. A switch initially functions as the root until it exchanges BPDUs with other switches. This exchange establishes which switch in the network is the root or root switch. If there is only one switch in the network, no exchange occurs, the forward-delay timer expires, and the interface moves to the listening state. An interface participating in spanning tree always enters the blocking state after switch initialization.

An interface in the blocking state performs these functions:

- Discards frames received on the interface
- Discards frames switched from another interface for forwarding
- Does not learn addresses
- Receives BPDUs

Listening State

The listening state is the first state a Layer 2 interface enters after the blocking state. The interface enters this state when the spanning tree decides that the interface should participate in frame forwarding.

An interface in the listening state performs these functions:

- Discards frames received on the interface
- Discards frames switched from another interface for forwarding
- Does not learn addresses
- Receives BPDUs

Learning State

A Layer 2 interface in the learning state prepares to participate in frame forwarding. The interface enters the learning state from the listening state.

An interface in the learning state performs these functions:

- Discards frames received on the interface
- Discards frames switched from another interface for forwarding
- Learns addresses
- Receives BPDUs

Forwarding State

A Layer 2 interface in the forwarding state forwards frames. The interface enters the forwarding state from the learning state.

An interface in the forwarding state performs these functions:

- Receives and forwards frames received on the interface
- Forwards frames switched from another interface
- Learns addresses
- Receives BPDUs

Disabled State

A Layer 2 interface in the disabled state does not participate in frame forwarding or in the spanning tree. An interface in the disabled state is non operational.

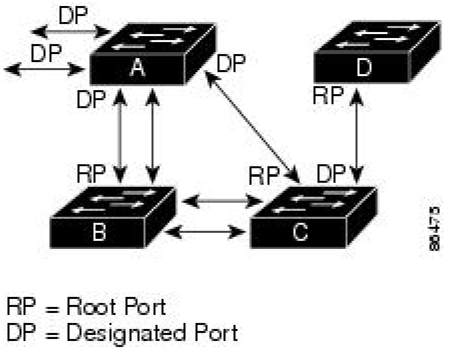
A disabled interface performs these functions:

- Discards frames received on the interface
- Discards frames switched from another interface for forwarding
- Does not learn addresses
- Does not receive BPDUs

How a Switch or Port Becomes the Root Switch or Root Port

If all switches in a network are enabled with default spanning-tree settings, the switch with the lowest MAC address becomes the root switch. In the figure below , Switch A is elected as the root switch because the switch priority of all the switches is set to the default (32768) and Switch A has the lowest MAC address. However, because of traffic patterns, number of forwarding interfaces, or link types, Switch A might not be the ideal root switch. By increasing the priority (lowering the numerical value) of the ideal switch so that it becomes the root switch, you force a spanning-tree recalculation to form a new topology with the ideal switch as the root.

Figure 12: Spanning-Tree Topology



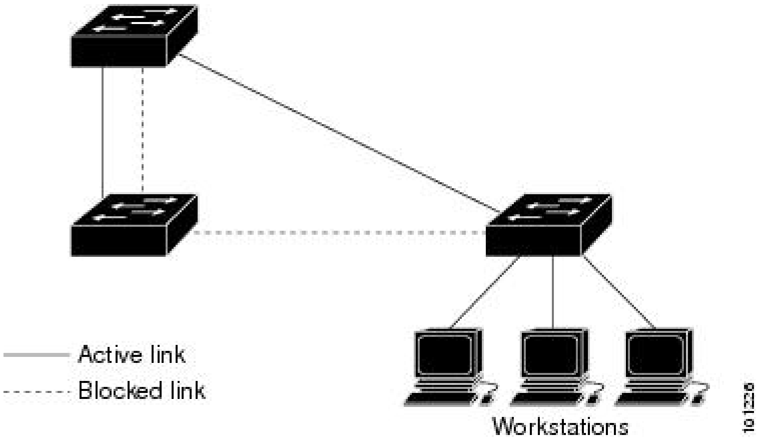
When the spanning-tree topology is calculated based on default parameters, the path between source and destination end stations in a switched network might not be ideal. For instance, connecting higher-speed links to an interface that has a higher number than the root port can cause a root-port change. The goal is to make the fastest link the root port.

For example, assume that one port on Switch B is a Gigabit Ethernet link and that another port on Switch B (a 10/100 link) is the root port. Network traffic might be more efficient over the Gigabit Ethernet link. By changing the spanning-tree port priority on the Gigabit Ethernet port to a higher priority (lower numerical value) than the root port, the Gigabit Ethernet port becomes the new root port.

Spanning Tree and Redundant Connectivity

You can create a redundant backbone with spanning tree by connecting two switch interfaces that are participating in spanning tree to another device or to two different devices, as shown in the figure below. Spanning tree automatically disables one interface but enables it if the other one fails. If one link is high-speed and the other is low-speed, the low-speed link is always disabled. If the speeds are the same, the port priority and port ID are added together, and spanning tree disables the link with the lowest value.

Figure 13: Spanning Tree and Redundant Connectivity



You can also create redundant links between switches by using EtherChannel groups.

Spanning-Tree Modes and Protocols

The following spanning-tree modes and protocols are supported:

- PVST+—This spanning-tree mode is based on the IEEE 802.1D standard and Cisco proprietary extensions. The PVST+ runs on each VLAN on the switch up to the maximum supported, ensuring that each has a loop-free path through the network.

  The PVST+ provides Layer 2 load balancing for the VLAN on which it runs. You can create different logical topologies by using the VLANs on your network to ensure that all of your links are used but that no one link is oversubscribed. Each instance of PVST+ on a VLAN has a single root switch. This root switch propagates the spanning-tree information associated with that VLAN to all other switches in the network. Because each switch has the same information about the network, this process ensures that the network topology is maintained.

- Rapid PVST+—This spanning-tree mode is the same as PVST+ except that is uses a rapid convergence based on the IEEE 802.1w standard. Rapid PVST+ is compatible with PVST+. To provide rapid convergence, the rapid PVST+ immediately deletes dynamically learned MAC address entries on a per-port basis upon receiving a topology change. By contrast, PVST+ uses a short aging time for dynamically learned MAC address entries.

  The rapid PVST+ uses the same configuration as PVST+ (except where noted), and the switch needs only minimal extra configuration. The benefit of rapid PVST+ is that you can migrate a large PVST+ install base to rapid PVST+ without having to learn the complexities of the MSTP configuration and without having to reprovision your network. In rapid-PVST+ mode, each VLAN runs its own spanning-tree instance up to the maximum supported.

- MSTP—This spanning-tree mode is based on the IEEE 802.1s standard. You can map multiple VLANs to the same spanning-tree instance, which reduces the number of spanning-tree instances required to support a large number of VLANs. The MSTP runs on top of the RSTP (based on IEEE 802.1w), which provides for rapid convergence of the spanning tree by eliminating the forward delay and by quickly transitioning root ports and designated ports to the forwarding state. You cannot run MSTP without RSTP.

  The most common initial deployment of MSTP is in the backbone and distribution layers of a Layer 2 switched network. For more information, see Multiple Spanning Tree Protocol chapter.

  For information about the number of supported spanning-tree instances, see Restrictions for PVST+ and RPVST+, on page 82.

Restrictions for PVST+ and RPVST+

- The Cisco NCS 520 routers support PVST+ and Rapid PVST+ (RPVST+) for only single tag encapsulation EFPs and trunk EFPs.

  There is no PVST and RPVST support for other encapsulations, such as a double tags, VLAN range, untag, and default.

- In PVST+ or rapid-PVST+ mode, the switch supports up to 128 spanning-tree instances.
- You must configure **l2protocol peer stp** command under all the EFP where you prefer to run STP.
- Port fast trunk works only if you configure it under interface mode and not under global mode.

- ROOT guard works only if you configure it under interface mode and not under global mode.

Spanning-Tree Interoperability and Backward Compatibility

The table below lists the interoperability and compatibility among the supported spanning-tree modes in a network.

Table 2: PVST+, MSTP, and Rapid-PVST+ Interoperability

	PVST+	MSTP	Rapid PVST+
PVST+	Yes	Yes (with restrictions)	Yes (reverts to PVST+)
MSTP	Yes (with restrictions)	Yes	Yes (reverts to PVST+)
Rapid PVST+	Yes (reverts to PVST+)	Yes (with restrictions)	Yes

In a mixed MSTP and PVST+ network, the common spanning-tree (CST) root must be inside the MST backbone, and a PVST+ switch cannot connect to multiple MST regions.

When a network contains switches running rapid PVST+ and switches running PVST+, we recommend that the rapid-PVST+ switches and PVST+ switches be configured for different spanning-tree instances. In the rapid-PVST+ spanning-tree instances, the root switch must be a rapid-PVST+ switch. In the PVST+ instances, the root switch must be a PVST+ switch. The PVST+ switches should be at the edge of the network.

Default Spanning-Tree Configuration

The table below shows the default spanning-tree configuration.

Table 3: Default Spanning-Tree Configuration

Feature	Default Setting
Enable state	Enabled on ports in VLAN 1.
Spanning-tree mode	Disabled.
Switch priority	32768.
Spanning-tree port priority (configurable on a per-interface basis)	128.
Spanning-tree port cost (configurable on a per-interface basis)	1000 Mbps: 4. 100 Mbps: 19. 10 Mbps: 100.
Spanning-tree VLAN port priority (configurable on a per-VLAN basis)	128.

Feature	Default Setting
Spanning-tree VLAN port cost (configurable on a per-VLAN basis)	1000 Mbps: 4. 100 Mbps: 19. 10 Mbps: 100.
Spanning-tree timers	Hello time: 2 seconds. Forward-delay time: 15 seconds. Maximum-aging time: 20 seconds.

Configuring PVST+ and RPVST+

The switch supports three spanning-tree modes: MSTP, PVST+, rapid PVST+.

Note By default, spanning-tree is disabled.

Use the following procedure to configure spanning-tree mode:

SUMMARY STEPS

1. **configure terminal**
2. **spanning-tree mode** {**pvst** | **rapid-pvst**
3. **spanning-tree vlan** *vlan-range*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree mode** {**pvst**	**rapid-pvst**	Configure a spanning-tree mode on STP ports on the switch. • Select **pvst** to enable PVST+. • Select **rapid-pvst** to enable rapid PVST+.
Step 3	**spanning-tree vlan** *vlan-range*	Configures STP on the range of VLAN specified.
Step 4	**end**	Return to privileged EXEC mode.

Configuring STP Peer Under EFP/TEFP

Beginning in privileged EXEC mode, follow these steps to configure the L2 protocol peer under EFP/TEFP. This procedure is optional.

SUMMARY STEPS

1. **configure terminal**
2. **interface TenGigabitEthernet***slot/subslot/port*
3. **no ip address**
4. **service instance trunk** *trunk id* **ethernet**
5. **encapsulation dot1q** *vlan-id*
6. **rewrite ingress tag pop 1 symmetric**
7. **l2protocol peer stp**
8. **bridge-domain from encapsulation**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** router#configure terminal	Enter global configuration mode.
Step 2	**interface TenGigabitEthernet***slot/subslot/port* **Example:** router(config)#interface TenGigabitEthernet0/0/27	Specifies the Gigabit Ethernet interface to configure. slot/subslot/port—Specify the location of the interface.
Step 3	**no ip address** **Example:** router(config-if)#no ip address	Disables the IP address on the interface.
Step 4	**service instance trunk** *trunk id* **ethernet** **Example:** router(config-if)#service instance trunk 1 ethernet	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.
Step 5	**encapsulation dot1q** *vlan-id* **Example:** router(config-if-srv)#encapsulation dot1q 1-100	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
Step 6	**rewrite ingress tag pop 1 symmetric** **Example:** router(config-if-serve)#rewrite ingress tag pop 1 symmetric	Specifies the encapsulation adjustment to be performed on a frame that is entering a service instance.
Step 7	**l2protocol peer stp** **Example:** router(config-if-srv)#l2protocol peer stp	Configures STP to peer with a neighbor on a port that has an EFP service instance.
Step 8	**bridge-domain from encapsulation** **Example:** router(config-if-srv)#bridge-domain from encapsulation	Configures support for EFPs on the interface.

	Command or Action	Purpose
Step 9	**end** **Example:** router(config-ip)# end	Returns to privileged EXEC mode.

Note You must configure **l2protocol peer stp** command under all the EFP where you prefer to run STP.

Disabling Spanning Tree

Disable spanning tree only if you are sure there are no loops in the network topology.

Caution When spanning tree is disabled and loops are present in the topology, excessive traffic and indefinite packet duplication can drastically reduce network performance.

Beginning in privileged EXEC mode, follow these steps to disable spanning-tree on a per-VLAN basis. This procedure is optional.

SUMMARY STEPS

1. **configure terminal**
2. **no spanning-tree vlan** *vlan-id*
3. **end**
4. **show spanning-tree vlan** *vlan-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no spanning-tree vlan** *vlan-id*	For *vlan-id* , the range is 1 to 4094.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree vlan** *vlan-id*	Verify your entries.

To re-enable spanning-tree, use the **spanning-tree vlan** *vlan-id* global configuration command.

Verifying PVST/RPVST Settings

Use the below commands to verify PVST and RPVST settings:

```
router#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     a89d.21ed.bbbd
             Cost        6
             Port        18 (GigabitEthernet0/0/11)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     b0aa.7754.553d
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  0   sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/0/7             Altn BLK 4         128.14   P2p
Gi0/0/11            Root FWD 4         128.18   P2p
```

```
router#show spanning-tree interface gigabitEthernet 0/0/7 detail

Port 14 (GigabitEthernet0/0/7) of VLAN0001 is alternate blocking
Port path cost 4, Port priority 128, Port Identifier 128.14.
Designated root has priority 32769, address a89d.21ed.bbbd
Designated bridge has priority 32769, address b0aa.7737.9dbd
Designated port id is 128.14, designated path cost 4
Timers: message age 4, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
BPDU: sent 91, received 8394
```

```
router#show spanning-tree summary

Switch is in pvst mode
Root bridge for: none
EtherChannel misconfig guard is enabled
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                      1         0        0          1          2
VLAN0002                      1         0        0          1          2
VLAN0003                      1         0        0          1          2
VLAN0004                      1         0        0          1          2
VLAN0005                      1         0        0          1          2
VLAN0006                      1         0        0          1          2
```

Configuring the Root Switch

The switch maintains a separate spanning-tree instance for each active VLAN configured on it. A bridge ID, consisting of the switch priority and the switch MAC address, is associated with each instance. For each VLAN, the switch with the lowest bridge ID becomes the root switch for that VLAN.

To configure a switch to become the root for the specified VLAN, use the **spanning-tree vlan** *vlan-id* **root** global configuration command to modify the switch priority from the default value (32768) to a significantly lower value. When you enter this command, the software checks the switch priority of the root switches for each VLAN. Because of the extended system ID support, the switch sets its own priority for the specified VLAN to 24576 if this value will cause this switch to become the root for the specified VLAN.

If any root switch for the specified VLAN has a switch priority lower than 24576, the switch sets its own priority for the specified VLAN to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value as shown in Table 14-1 on page 14-4 .)

Note The **spanning-tree vlan** *vlan-id* **root** global configuration command fails if the value necessary to be the root switch is less than 1.

If your network consists of switches that both do and do not support the extended system ID, it is unlikely that the switch with the extended system ID support will become the root switch. The extended system ID increases the switch priority value every time the VLAN number is greater than the priority of the connected switches running older software.

Note The root switch for each spanning-tree instance should be a backbone or distribution switch. Do not configure an access switch as the spanning-tree primary root.

Use the **diameter** keyword to specify the Layer 2 network diameter (that is, the maximum number of switch hops between any two end stations in the Layer 2 network). When you specify the network diameter, the switch automatically sets an optimal hello time, forward-delay time, and maximum-age time for a network of that diameter, which can significantly reduce the convergence time. You can use the **hello** keyword to override the automatically calculated hello time.

Note After configuring the switch as the root switch, we recommend that you avoid manually configuring the hello time, forward-delay time, and maximum-age time through the **spanning-tree vlan***vlan-id* **hello-time**, **spanning-tree vlan***vlan-id* **forward-time**, and the **spanning-tree vlan***vlan-id* **max-age** global configuration commands.

Beginning in privileged EXEC mode, follow these steps to configure a switch to become the root for the specified VLAN. This procedure is optional.

SUMMARY STEPS

1. **configure terminal**
2. **spanning-tree vlan** *vlan-id* **root primary** [**diameter** *net-diameter* [**hello-time** *seconds*]]
3. **end**
4. **show spanning-tree detail**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree vlan** *vlan-id* **root primary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	Configure a switch to become the root for the specified VLAN. • For *vlan-id* , you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. • (Optional) For **diameter** *net-diameter* , specify the maximum number of switches between any two end stations. The range is 2 to 7. • (Optional) For **hello-time** *seconds* , specify the interval in seconds between the generation of configuration messages by the root switch. The range is 1 to 10; the default is 2.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree detail**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no spanning-tree vlan** *vlan-id* **root** global configuration command.

Configuring a Secondary Root Switch

When you configure a switch as the secondary root, the switch priority is modified from the default value (32768) to 28672. The switch is then likely to become the root switch for the specified VLAN if the primary root switch fails. This is assuming that the other network switches use the default switch priority of 32768 and therefore are unlikely to become the root switch.

You can execute this command on more than one switch to configure multiple backup root switches. Use the same network diameter and hello-time values that you used when you configured the primary root switch with the **spanning-tree vlan** *vlan-id* **root primary** global configuration command .

Beginning in privileged EXEC mode, follow these steps to configure a switch to become the secondary root for the specified VLAN. This procedure is optional.

SUMMARY STEPS

1. **configure terminal**
2. **spanning-tree vlan** *vlan-id* **root secondary** [**diameter** *net-diameter* [**hello-time** *seconds*]]
3. **end**
4. **show spanning-tree detail**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree vlan** *vlan-id* **root secondary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	Configure a switch to become the secondary root for the specified VLAN. • For *vlan-id* , you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. • (Optional) For **diameter** *net-diameter* , specify the maximum number of switches between any two end stations. The range is 2 to 7. • (Optional) For **hello-time** *seconds* , specify the interval in seconds between the generation of configuration messages by the root switch. The range is 1 to 10; the default is 2. Use the same network diameter and hello-time values that you used when configuring the primary root switch. See Configuring the Root Switch.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree detail**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no spanning-tree vlan** *vlan-id* **root** global configuration command.

Configuring Port Priority

If a loop occurs, spanning tree uses the port priority when selecting a spanning-tree port to put into the forwarding state. You can assign higher priority values (lower numerical values) to ports that you want selected first and lower priority values (higher numerical values) to ones that you want selected last. If all spanning-tree ports have the same priority value, spanning tree puts the port with the lowest interface number in the forwarding state and blocks the other interfaces.

Beginning in privileged EXEC mode, follow these steps to configure the port priority of a spanning-tree port. This procedure is optional.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **spanning-tree port-priority** *priority*
4. **end**
5. Do one of the following:

- show spanning-tree interface *interface-id*
- **show spanning-tree vlan** *vlan-id*

6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify an interface to configure, and enter interface configuration mode. **Note** If the interface is a VLAN, only ports with spanning tree enabled in the VLAN will run spanning tree.If the interface is a port channel, all members of the port channel must be have spanning tree enabled.
Step 3	**spanning-tree port-priority** *priority*	Configure the port priority for the spanning-tree port. For *priority*, the range is 0 to 240, in increments of 16; the default is 128. Valid values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected. The lower the number, the higher the priority .
Step 4	**end**	Return to privileged EXEC mode.
Step 5	Do one of the following: • show spanning-tree interface *interface-id* • **show spanning-tree vlan** *vlan-id*	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Note The **show spanning-tree interface** *interface-id* privileged EXEC c ommand displays information only if the port is in a link-up operative state. Otherwise, you can use the **show running-config interface** privileged EXEC command to confirm the configuration.

To return to the default spanning-tree setting, use the **no spanning-tree** [**vlan** *vlan-id* **port-priority** interface configuration command.

Configuring Path Cost

The spanning-tree path cost default value is derived from the media speed of an interface (port running spanning tree or port channel of multiple ports running spanning tree). If a loop occurs, spanning tree uses cost when selecting an interface to put in the forwarding state. You can assign lower cost values to interfaces that you want selected first and higher cost values that you want selected last. If all NNIs (or port channels) have the same cost value, spanning tree puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.

Beginning in privileged EXEC mode, follow these steps to configure the cost of an interface. This procedure is optional.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **spanning-tree cost** *cost*
4. **end**
5. Do one of the following:
    - show spanning-tree interface *interface-id*
    - **show spanning-tree vlan** *vlan-id*
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify an interface to configure, and enter interface configuration mode. Valid interfaces include physical interfaces and port-channel logical interfaces (**port-channel** *port-channel-number*).
Step 3	**spanning-tree cost** *cost*	Configure the cost for an interface. If a loop occurs, spanning tree uses the path cost when selecting an interface to place into the forwarding state. A lower path cost represents higher-speed transmission. For *cost*, the range is 1 to 200000000; the default value is derived from the media speed of the interface.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	Do one of the following: • show spanning-tree interface *interface-id* • **show spanning-tree vlan** *vlan-id*	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Note The **show spanning-tree interface** *interface-id* privileged EXEC c ommand displays information only for ports that are in a link-up operative state. Otherwise, you can use the **show running-config** privileged EXEC co mmand to confirm the configuration.

To return to the default setting, use the **no spanning-tree** [**vlan** *vlan-id*] **cost** interface configuration command.

Configuring the Switch Priority of a VLAN

You can configure the switch priority and make it more likely that the switch will be chosen as the root switch.

Note Exercise care when using this command. For most situations, we recommend that you use the **spanning-tree vlan** *vlan-id* **root primary** and the **spanning-tree vlan** *vlan-id* **root secondary** global configuration commands to modify the switch priority.

Beginning in privileged EXEC mode, follow these steps to configure the switch priority of a VLAN. This procedure is optional.

SUMMARY STEPS

1. **configure terminal**
2. **spanning-tree vlan** *vlan-id* **priority** *priority*
3. **end**
4. **show spanning-tree vlan** *vlan-id*
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree vlan** *vlan-id* **priority** *priority*	Configure the switch priority of a VLAN. • For *vlan-id* , you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. • For *priority*, the range is 0 to 61440 in increments of 4096; the default is 32768. The lower the number, the more likely the switch will be chosen as the root switch. Valid priority values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree vlan** *vlan-id*	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no spanning-tree vlan** *vlan-id* **priority** global configuration command.

Configuring Spanning-Tree Timers

Table 4: Spanning-Tree.Timers

Variable	Description
Hello timer	Controls how often the switch broadcasts hello messages to other switches.
Forward-delay timer	Controls how long each of the listening and learning states last before the STP port begins forwarding.
Maximum-age timer	Controls the amount of time the switch stores protocol information received on an STP port.

Configuring the Hello Time

You can configure the interval between the generation of configuration messages by the root switch by changing the hello time.

Note Exercise care when using this command. For most situations, we recommend that you use the **spanning-tree vlan** *vlan-id* **root primary** and the **spanning-tree vlan** *vlan-id* **root secondary** global configuration commands to modify the hello time.

Beginning in privileged EXEC mode, follow these steps to configure the hello time of a VLAN. This procedure is optional.

SUMMARY STEPS

1. **configure terminal**
2. **spanning-tree vlan** *vlan-id* **hello-time** *seconds*
3. **end**
4. **show spanning-tree vlan** *vlan-id*
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree vlan** *vlan-id* **hello-time** *seconds*	Configure the hello time of a VLAN. The hello time is the interval between the generation of configuration messages by the root switch. These messages mean that the switch is alive. • For *vlan-id*, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated

	Command or Action	Purpose
		by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. • For *seconds* , the range is 1 to 10; the default is 2.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree vlan** *vlan-id*	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no spanning-tree vlan** *vlan-id* **hello-time** global configuration command.

Configuring the Forwarding-Delay Time for a VLAN

Beginning in privileged EXEC mode, follow these steps to configure the forwarding-delay time for a VLAN. This procedure is optional.

SUMMARY STEPS

1. **configure terminal**
2. **spanning-tree vlan** *vlan-id* **forward-time** *seconds*
3. **end**
4. **show spanning-tree vlan** *vlan-id*
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree vlan** *vlan-id* **forward-time** *seconds*	Configure the forward time of a VLAN. The forward delay is the number of seconds a spanning-tree port waits before changing from its spanning-tree learning and listening states to the forwarding state. • For *vlan-id*, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. • For *seconds* , the range is 4 to 30; the default is 15.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree vlan** *vlan-id*	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no spanning-tree vlan** *vlan-id* **forward-time** global configuration command.

Configuring the Maximum-Aging Time for a VLAN

Beginning in privileged EXEC mode, follow these steps to configure the maximum-aging time for a VLAN. This procedure is optional.

SUMMARY STEPS

1. **configure terminal**
2. **spanning-tree vlan** *vlan-id* **max-age** *seconds*
3. **end**
4. **show spanning-tree vlan** *vlan-id*
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree vlan** *vlan-id* **max-age** *seconds*	Configure the maximum-aging time of a VLAN. The maximum-aging time is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration. • For *vlan-id*, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. • For *seconds* , the range is 6 to 40; the default is 20.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree vlan** *vlan-id*	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no spanning-tree vlan** *vlan-id* **max-age** global configuration command.

Displaying the Spanning-Tree Status

To display the spanning-tree status, use one or more of the privileged EXEC commands in the table below:

Table 5: Commands for Displaying Spanning-Tree Status

Command	Purpose
show spanning-tree active	Displays spanning-tree information only on active spanning-tree interfaces.

Command	Purpose
show spanning-tree detail	Displays a detailed summary of interface information.
show spanning-tree interface *interface-id*	Displays spanning-tree information for the specified spanning-tree interface.
show spanning-tree summary totals	Displays a summary of interface states or displays the total lines of the STP state section.

You can clear spanning-tree counters by using the **clear spanning-tree** [**interface***interface-id*] privileged EXEC command.

For information about other keywords for the **show spanning-tree** privileged EXEC command, see the command reference for this release.