Resilient Ethernet Protocol (REP)

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.

- Finding Feature Information, page 1
- Restrictions for Resilient Ethernet Protocol, page 1
- Information About REP, page 2
- How to Configure REP, page 10
- Configuration Examples for REP, page 24
- Additional References, page 26
- Feature Information for Resilient Ethernet Protocol, page 27

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.

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 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.
- The recommended minimum REP LSL timer value is 200 ms.
- The REP ports are removed from the topology list during the following situations:
  - 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.

  It is designed to avoid the traffic loop based on the above behavior to adopt dynamic REP configuration changes.

Information About REP

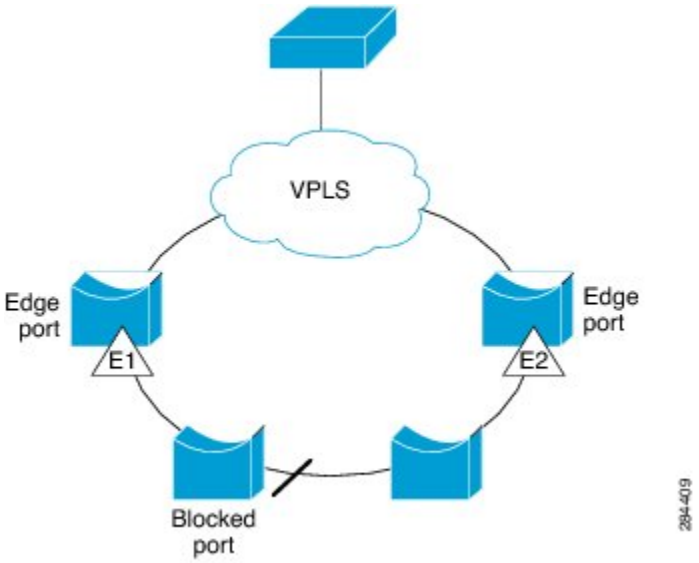
REP Segments

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.

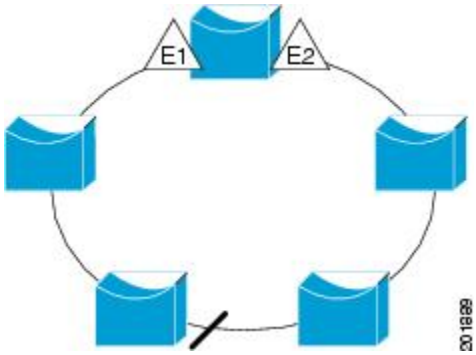
Figure 1: REP Open Segments



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.

REP Integrated with VPLS

Normally, in a Virtual Private LAN Service (VPLS) network core, all nodes are connected in a full-mesh topology and each node has connectivity to all other nodes. In the full-mesh topology, there is no need for a node to retransmit data to another node. In Figure 3, the common ring provides a path where the packet can be forwarded to another network provider edge (N-PE) router, breaking split horizon model.

REP emulates a common link connection the REP ring supports the VPLS full-mesh model, but maintains the split horizon properties so the super-loop does not exist. The emulated common link uses the Clustering over the WAN (CWAN) line card, which is also used for the VPLS uplink. This emulated common link forwards data from the ring to either the VPLS uplink or to the other side of the ring; blocks data coming from the VPLS core network; and handles access to pseudowire for Hierarchical-VPLS (H-VPLS) topologies.

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 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 22 REP segments per 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 903 Series Routers. Trunk EFP ports can have several bridged VLAN services running on them. 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.

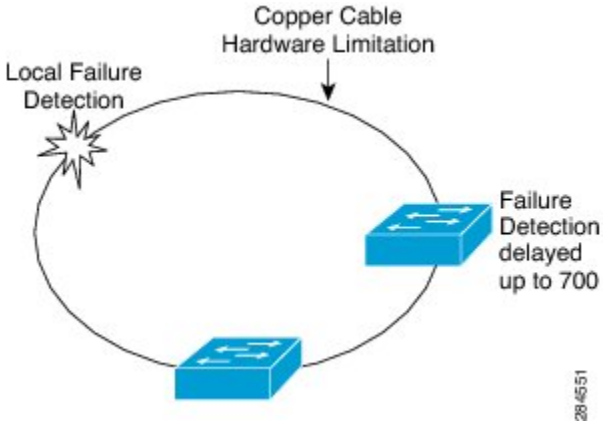
REP Configurable Timers

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 200-10000 ms to receive LSL frames. If no LSL frames are received from 200 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



SSO Support for REP Fast Hello

When a router crashes, it takes between 3 to 5 seconds for the router to get into active mode and start sending REP Fast Hello packets. If the value of the age out timer configured by the **lsl age out timer** command is less than 3 seconds, the remote end detects a port failure and reconverges. After reconverging, the router sends out a BPDU with a special type, length, and, value (TLV) to the connected port. The router learns the port's local and remote sequence number so that the subsequent REP three-way link integrity check does not fail. The Stateful Switchover (SSO) support for REP ensures that a Fast Hello packet can be sent from the router before the LSL interval expires.

REP Edge No-Neighbor Support

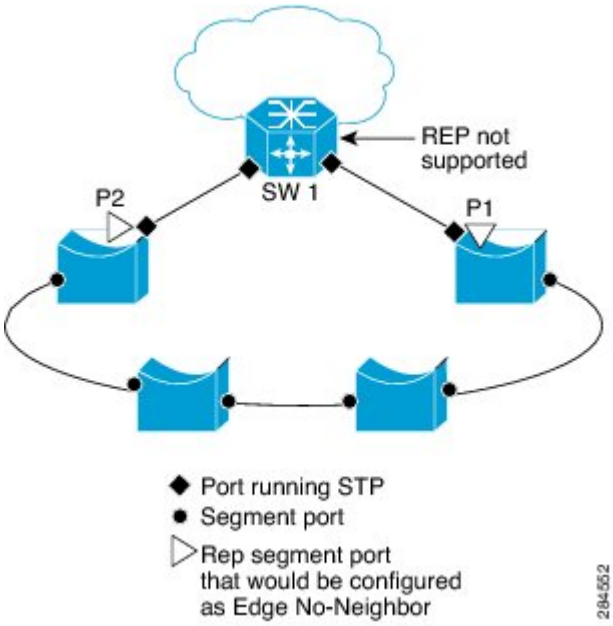
In a ring network topology, aggregation nodes do not support REP. A REP segment can be created with no-neighbor ports to achieve convergence of switches. The figure below shows P1 and P2 as Edge No-Neighbor ports in a ring topology. In this configuration P1 and P2 can block traffic. If there is a failure 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



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 gigabitethernet0/1 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 vlan 10`	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 20.

	Command or Action	Purpose
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.
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**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• 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. **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.

	Command or Action	Purpose
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 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**]	(Optional) Verifies the REP interface configuration. • Enter the interface type and number and the optional **detail** keyword, if desired.

	Command or Action	Purpose
	Example: `Router# show interface Gigabitethernet0/0/1 rep detail`	
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. **configure terminal**
3. **rep preempt segment** *segment-id*
4. **end**
5. **show rep topology**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**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.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 5	**show rep topology** **Example:** `Router# show rep topology`	Displays the REP topology information.

Configuring SNMP Traps for REP

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp mib rep trap-rate** *value*
4. **end**
5. **show running-config**
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	**snmp mib rep trap-rate** *value* **Example:** `Router(config)# snmp mib rep trap-rate 500`	Enables the router to send REP traps, and sets the number of traps sent per second. • Enter the number of traps sent per second. The range is from 0 to 1000. The default is 0 (no limit imposed; a trap is sent at every occurrence). **Note** To remove the traps, enter the **no snmp mib rep trap-rate** command.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Router# show running-config`	(Optional) Displays the running configuration, which van be used to verify the REP trap configuration.
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the router startup configuration file.

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 gigabitethernet0/1 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.

	Command or Action	Purpose
		• (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 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. **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.

	Command or Action	Purpose
		• 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. We recommend that you configure the minimum range as 200 for better performance. While a lower value can help improve performance, any changes to this command must be carefully evaluated. Lowering the value indiscriminately may destabilize the system.
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.
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. • (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.

	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.

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

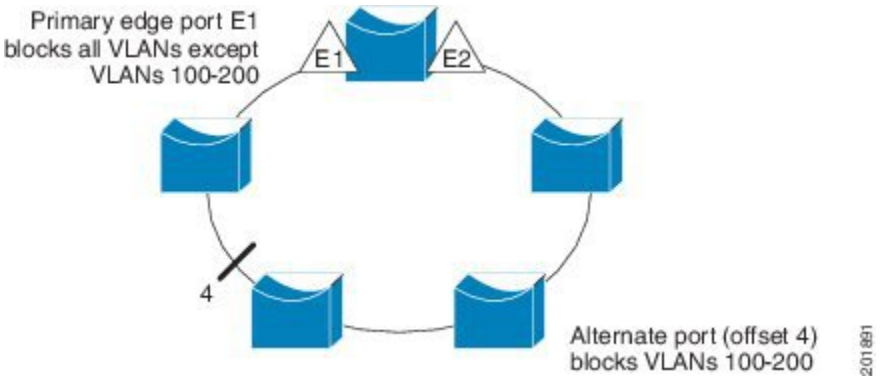
This example shows how to configure REP support on a Trunk EFP. An interface is configured as the primary edge port for segment 1 to send STCNs to segments 2 through 5; the alternate port is configured as the port with port ID 0009001818D68700 to block all VLANs after a preemption delay of 60 seconds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

Figure 5: Example of VLAN Blocking




```
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# configure terminal
Router(config)rep preempt segment 1
Router(config)# end
```

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

GigabitEthernet0/1 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 GigabitEthernet0/2
Router(config-if)# rep segment t1 edge no-neighbor primary
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
LAN Switching commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples.	Cisco IOS LAN Switching Command Reference
Introduction to spanning tree protocols	Spanning Tree Protocol (STP)/802.1D
Spanning Tree PortFast BPDU Guard Enhancement feature	Spanning Tree PortFast BPDU Guard Enhancement

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Resilient Ethernet Protocol

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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.

Table 1: Feature Information for Resilient Ethernet Protocol

Feature Name	Releases	Feature Information
REP Configurable Timers	Cisco IOS XE Release 3.5.1S	REP Configurable Timers on REP to detect link failures in a link between routers in a ring topology. In Cisco IOS XE Release 3.5.1S, support was added for the Cisco ASR 903 Router. In Cisco IOS XE Release 3.11S, support was added for the Cisco ASR 901 Routers. The following sections provide information about this feature: REP Configurable Timers Configuring REP Configurable Timers Configuring REP Configurable Timers

Feature Name	Releases	Feature Information
REP Edge No-Neighbor Support	Cisco IOS XE Release 3.5.1S	The Edge No-Neighbor Support on REP enables defining a new type of edge that has an internal neighbor. In Cisco IOS XE Release 3.5.1S, support was added for the Cisco ASR 903 Router. REP Edge No-Neighbor Support Configuring REP Edge No-Neighbor Support
REP Support on Trunk EVC	Cisco IOS XE Release 3.5S	REP can be configured on Trunk Ethernet Flow Point (EFP) ports at an interface level on ASR 903 Series Routers. The following command was introduced by this feature: **service instance trunk**.
SSO Support for REP Fast Hello	Cisco IOS XE Release 3.5.1S	SSO Support for REP Fast Hello is provided to ensure that a Fast Hello packet is sent from an active router before the LSL timeout interval expires. In Cisco IOS XE Release 3.5.1S, support was added for the Cisco ASR 903 Router. In Cisco IOS XE Release 3.11S, support was added for the Cisco ASR 901 Router. The following sections provide information about this feature: SSO Support for REP Fast Hello