



## How to Configure REP

---

- [Configuring the REP Administrative VLAN, on page 1](#)
- [Configuring REP Interfaces, on page 1](#)
- [Configuring REP Negotiated, on page 3](#)
- [Setting Manual Preemption for VLAN Load Balancing, on page 5](#)
- [Configuring SNMP Traps for REP, on page 6](#)
- [Configuring REP ZTP, on page 6](#)
- [Configuring REP Segment-ID Autodiscovery, on page 7](#)

### Configuring the REP Administrative VLAN

To configure the REP administrative VLAN, enter the following commands:

---

**Step 1** Enter global configuration mode:

```
configure terminal
```

**Step 2** Specify the administrative VLAN:

```
rep admin vlan vlan-id
```

The range is 2 to 4096. The default is VLAN 1. To set the admin VLAN to 1, enter the **no rep admin vlan** global configuration command.

**Step 3** Return to privileged EXEC mode:

```
end
```

---

### Configuring REP Interfaces

#### Before you begin

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

**Step 1** Enter global configuration mode:

```
configure terminal
```

**Step 2** Specify the interface, and enter interface configuration mode:

```
interface interface-id
```

The interface can be a physical Layer 2 interface or a port channel (logical interface). The port-channel range is 1 to 10.

**Step 3** Configure the interface as a Layer 2 trunk port:

```
switchport mode trunk
```

**Step 4** Enable REP on the interface, and identify a segment number:

```
rep segment segment-id [edge [no-neighbor] [primary]] [preferred]
```

The segment ID range is from 1 to 1024. These optional keywords are available:

**Note** You must configure two edge ports, including one primary edge port for each segment.

- **edge** —Configures the port as an edge port. Entering **edge** without the **primary** keyword configures the port as the secondary edge port. Each segment has only two edge ports.
- (Optional) **primary** — Configures the port as the primary edge port, the port on which you can configure VLAN load balancing.
- (Optional) **no-neighbor**— Configures a port with no external REP neighbors as an edge port. The port inherits all properties of edge ports, and you can configure them the same as any edge port.

**Note** Although each segment can have only one primary edge port, if you configure edge ports on two different switches and enter the **primary** keyword on both switches, the configuration is allowed. 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 it a slight edge among equal contenders. The alternate port is usually a previously failed port.

**Step 5** (Optional) Configure the edge port to send segment topology change notices (STCNs):

```
rep stcn {interface interface-id | segment id-list | stp }
```

- **interface interface-id** —Designates a physical interface or port channel to receive STCNs.
- **segment id-list**— Identifies one or more segments to receive STCNs. The range is 1 to 1024.
- **stp**— Sends STCNs to STP networks.

**Step 6** (Optional) Configure VLAN load balancing on the primary edge port, identify the REP alternate port in one of three ways, and configure the VLANs to be blocked on the alternate port.

```
rep block port {id port-id | neighbor_offset |preferred} vlan {vlan-list | all}
```

- **id** *port-id*—Identifies the alternate port by port ID. The port ID is automatically generated for each port in the segment. You can view interface port IDs by entering the **show interface interface-id rep [ detail ]** privileged EXEC command.
- **neighbor\_offset** number—Identifies 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. See [VLAN Load Balancing](#) for an example of neighbor offset numbering.

**Note** Because you enter this command at the primary edge port (offset number 1), you would never enter an offset value of 1 to identify an alternate port.

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

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

**Step 7** (Optional) You must enter this command and configure a preempt time delay if you want VLAN load balancing to automatically trigger after a link failure and recovery.

```
rep preempt delay seconds
```

The time delay range is 15 to 300 seconds. The default is manual preemption with no time delay.

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

**Step 8** (Optional) Configure a time (in milliseconds) for which the REP interface remains up without receiving a hello from a neighbor.

```
rep lsl-age-timer value
```

The range is from 120 to 10000 ms in 40-ms increments. The default is 5000 ms (5 seconds).

**Note** If the neighbor device is not running Cisco IOS Release 12.2(52)SE or later, it only accepts values from 3000 to 10000 ms in 500-ms intervals. EtherChannel port channel interfaces do not support LSL age-timer values less than 1000 ms.

**Step 9** Return to privileged EXEC mode:

```
end
```

---

## Configuring REP Negotiated

Use the following procedure to configure REP Negotiated in a REP network where a new switch is being inserted into the existing REP ring topology. The adjacent switches to this newly inserted switch are referred to as peer switches.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	On the new switch, configure <b>rep bpduleak</b> in global configuration mode:	<code>rep bpduleak</code> !
<b>Step 2</b>	<p>Configure the EEM macros on the new switch as shown in the following example. This example assumes that the peer switches are configured with REP Segment 777 and the newly inserted switch has uplink ports GigabitEthernet 1/1 and GigabitEthernet 1/2.</p> <p><b>Example:</b></p> <pre>macro auto execute CISCO_REP_NEG_EVENT {   config terminal   no rep bpduleak   interface GigabitEthernet 1/1   switchport mode trunk   no rep negotiated   rep segment 777   interface GigabitEthernet 1/2   switchport mode trunk   no rep negotiated   rep segment 777   exit }  macro auto execute CISCO_REP_NONNEG_EVENT {   config terminal   no rep bpduleak   interface GigabitEthernet 1/1   no rep negotiated   interface GigabitEthernet 1/2   no rep negotiated } !</pre>	
<b>Step 3</b>	Insert the new switch into the existing REP Ring topology.	<b>Note</b> The newly inserted switch still does not have any REP Segment configurations.
<b>Step 4</b>	Check the output of <b>show rep topology</b> on the peer switches.	The output should show that <b>rep bpduleak</b> is in effect. The REP segment remains intact, but the newly inserted switch is not reflected in the topology. This indicates that the newly inserted switch is transparently forwarding the REP traffic between its uplink ports.
<b>Step 5</b>	<p>Configure <b>rep negotiated</b> on both the uplink interfaces of the newly inserted switch.</p> <p><b>Example:</b></p> <pre>interface range GigabitEthernet 1/1-2   rep negotiated !</pre>	
<b>Step 6</b>	<p>Use the <b>show rep negotiated</b> command on the newly inserted switch to verify the status.</p> <p><b>Example:</b></p>	

	Command or Action	Purpose
	<pre>Switch2 #show rep negotiated REP negotiation status : Fail  Interface1: GigabitEthernet1/1 Status : enabled Rx State : fail, Segment-ID: 0  Interface2: GigabitEthernet1/2 Status : enabled Rx State : fail, Segment-ID: 0</pre>	
<b>Step 7</b>	<p>Configure <b>rep negotiated</b> on the connected uplink interfaces of both the peer switches and wait for the REP Negotiation to complete. The following console log message on the newly inserted switch indicates that an EEM event has been triggered by REP Negotiation.</p> <p><b>Example:</b></p> <pre>May 22 22:54:41.087: REP negotiated event generated, executed CISCO_REP_NEG for Segment 777</pre>	
<b>Step 8</b>	<p>Use the <b>show rep negotiated</b> command on the newly inserted switch to verify the status.</p> <p><b>Example:</b></p> <pre>Switch2#show rep negotiated REP negotiation status : Success  Interface1: GigabitEthernet1/1 Status : disabled  Interface2: GigabitEthernet1/2 Status : disabled</pre>	<p>REP is configured automatically in the newly inserted switch and it also appears in the <b>show rep topology</b> output on all the switches in the REP Ring.</p>

## Setting Manual Preemption for VLAN Load Balancing

### Before you begin

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

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	Manually trigger VLAN load balancing on the segment:	<pre>rep preempt segment segment-id</pre> <p>You will need to confirm the command before it is executed.</p>
<b>Step 2</b>	Display REP topology information:	<pre>show rep topology</pre>

## Configuring SNMP Traps for REP

You can configure the switch to send REP-specific traps to notify the SNMP server of link operational status changes and port role changes.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	Enter global configuration mode:	<code>configure terminal</code>
<b>Step 2</b>	Enable the switch to send REP traps, and set the number of traps sent per second:	<code>snmp mib rep trap-rate value</code> The range is from 0 to 1000. The default is 0 (no limit imposed; a trap is sent at every occurrence).
<b>Step 3</b>	Return to privileged EXEC mode:	<code>end</code>

## Configuring REP ZTP

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

- Global level: Enabled
- Interface level: Disabled

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



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

**Step 1** Enter global configuration mode:

```
Switch# configure terminal
```

**Step 2** Globally enable REP ZTP:

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

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

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

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

**Step 4** Enable REP ZTP on the interface:

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

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

---

### Example

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

```
Switch#show running-config interface gigabitEthernet 1/2
Building configuration...

Current configuration : 93 bytes
!
interface GigabitEthernet1/2
 switchport mode trunk
 rep segment 100
 rep ztp-enable
end
```

## Configuring REP Segment-ID Autodiscovery

You use CLI commands for REP Segment-ID Autodiscovery. One enables or disables autodiscovery on a REP switch, and one configures new interfaces so the switch learns the segment-ID. You also use CLI commands to view the status of the feature on the segment.

### Enable REP Segment-ID Autodiscovery

REP Segment-ID Autodiscovery is enabled by default. However, you can re-enable it on the switch upstream and downstream interfaces.

---

Enable REP Segment-ID Autodiscovery on the switch.

#### Example:

```
switch(config)#rep autodisc
```

You disable REP Segment-ID Autodiscovery by entering the following command:

```
switch(config)#no rep autodisc
```

---

#### What to do next

You can check the status of REP Segment-ID Autodiscovery. See the section [View REP Segment ID Autodiscovery Status](#) in this guide.

## Configure the Interfaces

Configure the interface on the newly inserted switch to enable REP Segment-ID learning. This configuration command is available on all uplink and downlink ports.

### Before you begin

Ensure that the REP segment ID is configured on the primary and secondary edge devices. You configure the segment ID by entering the command **rep segment *segment\_id* edge**, in which *segment\_id* is the segment ID of the ring to be propagated through CDP packet to the neighboring device when connected.

---

Enable the switch to learn the segment ID.

### Example:

```
switch(config)#int gig1/1
switch(config-if)#rep seg auto
```

This command is not reflected in the "running-config" of the switch until the REP Segment-ID learning is completed successfully. The learned REP Segment-ID is cached internally. This cached information is used whenever available instead of learning the REP Segment-ID from the Peer switch. Any previously configured REP Segment-ID configuration automatically gets cached when `rep segment auto` is configured on an interface.

The following example shows the minimum configuration to enable the feature on an interface on the upstream device switch. The upstream device with an explicit REP segment is typically an edge switch.

```
switch#show running-config interface gigabitEthernet 1/3
Building configuration...
```

```
Current configuration : 93 bytes
!
interface GigabitEthernet1/3
 switchport mode trunk
 rep segment auto 1
```

The following example shows the minimum configuration to enable the feature on an interface on the downstream switch interface. Enter the command **show running-config interface *interface\_id*** to confirm that the downstream switch knows to expect to receive its REP segment through CDP message.

```
switch#show running-config interface gigabitEthernet 1/2
Building configuration...
```

```
Current configuration : 93 bytes
!
interface GigabitEthernet1/2
 switchport mode trunk
 rep segment auto
end
```

You disable the ability of the switch to learn the segment ID by entering the following command:

```
switch(config-if)#no rep segment
```

---

### What to do next

You can check the status of REP Segment-ID Autodiscovery. See the section [View REP Segment ID Autodiscovery Status](#) in this guide.