REP Access Gateway

Resilient Ethernet Protocol (REP) is a Cisco proprietary protocol that provides an alternative to the Spanning Tree Protocol (STP). REP provides fast reconvergence and traffic recovery when a link in a ring fails. Fast reconvergence is achieved by notifying all nodes in the ring with a control message that activates the redundant path to the core network.

The REP Access Gateway Enhancements feature allows fast failure detection notifications between devices configured with REP access gateway (REP-AG), by enabling communication between Connectivity Fault Manager (CFM) and REP.

Restrictions for REP Access Gateway Enhancements

- EFD is only supported on physical ports and services; it is not supported on VLAN sub interfaces.

- The CCM interval for CMF service on which EFD is supported is limited by the platform capabilities.

- The EFD feature is only supported on Down MEPs.

- EFD is not supported on trunk services.

- EFD is not supported for both G-8032 and REP at the same time.

- Only one MEP on a given interface or EFP may be configured for EFD. You cannot have MEPs operating at multiple CFM levels on the same interface.

Information About REP Access Gateway Enhancements

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 Enhancements

Configuring REP Access Gateway Enhancements

Perform this task to configure EFD messages to REP devices.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm global**
4. **link-protection enable**
5. **link-protection group management vlan** *vlan-id*
6. **link-protection group** *group-number* **pccm vlan** *vlan-id*
7. **ethernet cfm domain** *domain-name***level** *level-id* [**direction outward**]
8. **service** { *ma-name* | *ma-number* | **vlan-id** *vlan-id* | **vpn-id** *vpn-id* } [**port** | **vlan** *vlan-id* [**direction** *down*]]
9. **continuity-check**
10. **continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**]
11. **efd notify rep**
12. **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:**	Enables Ethernet CFM globally.

	Command or Action	Purpose
	`Device(config)# ethernet cfm global`	
Step 4	**link-protection enable** **Example:** `Device(config)# link-protection enable`	Enables link protection globally on the router.
Step 5	**link-protection group management vlan** *vlan-id* **Example:** `Device(config)# link-protection group management vlan 51`	Defines the management VLAN used for link protection.
Step 6	**link-protection group** *group-number* **pccm vlan** *vlan-id* **Example:** `Device(config)# link-protection group 2 pccm vlan 16`	Specifies an ODU-to-ODU continuity check message (P-CCM) VLAN.
Step 7	**ethernet cfm domain** *domain-name***level** *level-id* [**direction outward**] **Example:** `Device(config)# ethernet cfm domain REP_domain level 4`	Configures the CFM domain for ODU 1 and enters Ethernet CFM configuration mode.
Step 8	**service** { *ma-name* | *ma-number* |**vlan-id** *vlan-id* |**vpn-id** *vpn-id* } [**port** | **vlan** *vlan-id* [**direction** *down*]] **Example:** `Device(config-ecfm)# service rep_service evc rep-evc vlan 1001 direction down`	Defines a maintenance association for ODU 1 and enters Ethernet CFM service instance configuration mode.
Step 9	**continuity-check** **Example:** `Device(config-ecfm)# continuity-check`	Enables CCM message transmission.
Step 10	**continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**] **Example:** `Device(config)# Device(config-ecfm-srv)# continuity-check interval 3.3ms`	Configures the time period between CCM message transmissions
Step 11	**efd notify rep** **Example:** `Device(config-ecfm-srv)# efd notify rep`	Enables EFD notifications to REP devices.
Step 12	**end** **Example:** `Device(config-ecfm-srv)# end`	Returns to user EXEC mode.

Verifying REP Access Gateway Enhancements

Perform this optional task to verify the status of interface monitored for EFD.

SUMMARY STEPS

1. **enable**
2. **show interface** *number* **rep detail**

DETAILED STEPS

Step 1   **enable**

Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
device> enable
```

Step 2   **show interface** *number* **rep detail**

Use this command to verify that EFD is enabled for REP devices:

Example:

```
device# show interface ethenet 0/0/1 rep detail
GigabitEthernet1/7   REP enabled
Segment-id: 10 (Primary Edge No-Neighbor)
PortID: 0007001AE3DC2680
Preferred flag: Yes
EFD Status: Enabled
EFD State: Fault/Clear
Operational Link Status: NO_NEIGHBOR
Current Key: 0007001AE3DC26806BD6
Port Role: Alternate
Blocked VLAN: 30-40
Admin-vlan: 500
```

Configuration Examples For REP Access Gateway Enhancements

Example Configuring REP Access Gateway Enhancements

This example shows how to configure EFD messages for REP devices.

```
Device> enable
Device# configure terminal
Device(config)# ethernet cfm global
Device(config)# link-protection enable
Device(config)# link-protection group management vlan 51
Device(config)# link-protection group 2 pccm vlan 16
```

```
Device(config)# ethernet cfm domain REP_domain level 4
Device(config-ecfm)# service rep_service evc rep-evc vlan 1001 direction down
Device(config-ecfm-srv)# continuity-check
Device(config-ecfm-srv)# continuity-check interval 3.3ms
Device(config-ecfm-srv)# efd notify rep
Device(config-ecfm-srv)# end
```

Feature Information for REP Access Gateway Enhancement

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 Access Gateway Enhancements	Cisco IOS XE Release 3.13	The REP Access Gateway Enhancements feature allows fast failure detection notifications between devices configured with REP access gateway (REP-AG), by enabling communication between Connectivity Fault Manager (CFM) and REP. The following commands were introduced by this feature: **efd notify rep** .