Configuring Ethernet Ring Protection

This chapter describes how to configure Ethernet Ring Protection on the Cisco ME 3800X, ME 3600X, and ME3600X-24CX switches.

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, page 62-1
- Restrictions and Limitations, page 62-1
- Information About Ethernet Ring Protection Switching, page 62-2
- How to Configure ITU-T G.8032 Ethernet Ring Protection Switching, page 62-8
- Configuration Examples for Ethernet Ring Protection Switching, page 62-11

Configuration information for Ethernet Ring Protection Switching can be found in ITU-T G.8032 Ethernet Ring Protection Switching section.


Prerequisites

- The Ethernet Flow Points (EFPs) must be configured.

Restrictions and Limitations

The following restriction apply to Cisco ME3600X/ME3800X switch.

- It is not possible to block some encapsulation VLANs and unblock the remaining encapsulation VLANs on a single EVC. Therefore you must block or unblock entire EVCs.
  
  When configuring EVCs:
  
  - EVCs that contain the inclusion-list VLANs should not contain any other VLANs in the encapsulation list
  - If load-balancing is required an additional EVC should be used.
  - G8032 Feature is supported only on EVC. It is not supported on switchport.
- ITU-T G.8032 sub-ring with virtual-channel is not supported.
- ITU-T G.8032 is not supported on Port-channel.
- Support for a maximum of two ERP instance per ring.
- Trunk EFP is not supported
- TCN propagation is only supported from ITU-T G.8032 Minor Ring to ITU-T G.8032 Major Ring. TCN propagation from ITU-T G.8032 to MST or REP is not supported.
- The switch supports a maximum of eight ITU-T G.8032 Rings.
- ITU-T G.8032 Feature with CFM is supported with a CFM interval of 3.3ms/10ms/100ms.
- VLANs that are used for the R-APS control channel cannot be reused for Data traffic.

Information About 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.
Chapter 62 Configuring Ethernet Ring Protection

Information About Ethernet Ring Protection Switching

Figure 62-1

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 3.3/10/100 milliseconds (ms). At this interval (which is supported only on ME3600X-24CX platform), 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:
Information About Ethernet Ring Protection Switching

- 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
  - Multiple MS commands cancel all MS commands

- 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.

- 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.
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.
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.
Ethernet Flow Points

An Ethernet flow point (EFP) is a forwarding decision point in the provider edge (PE) router, which gives network designers flexibility to make many Layer 2 flow decisions within the interface. Many EFPs can be configured on a single physical port. (The number varies from one device to another.) EFPs are the logical demarcation points of an Ethernet virtual connection (EVC) on an interface. An EVC that uses two or more user network interfaces (UNIs) requires an EFP on the associated ingress and egress interfaces of every device that the EVC passes through.

EFPs can be configured on any Layer 2 traffic port; however, they are usually configured on UNI ports. The following parameters (matching criteria) can be configured on the EFP:

- Frames of a specific VLAN, a VLAN range, or a list of VLANs (100-150 or 100,103,110)
- Frames with no tags (untagged)
- Frames with identical double-tags (VLAN tags) as specified
- Frames with identical Class of Service (CoS) values

A frame passes each configured match criterion until the correct matching point is found. If a frame does not fit any of the matching criteria, it is dropped. Default criteria can be configured to avoid dropping frames.

The following types of commands can be used in an EFP:

- Rewrite commands—In each EFP, VLAN tag management can be specified with the following actions:
  - Pop—1) pops out a tag; 2) pops out two tags
  - Push—1) pushes in a tag; 2) pushes in two tags
  - Translate—1 to 1) changes a tag value; 1 to 2) pops one tag and pushes two tags; 2 to 1) pops two tags and pushes one tag; 2 to 2) changes the value for two tags.

- Forwarding commands—Each EFP specifies the forwarding command for the frames that enter the EFP. Only one forwarding command can be configured per EFP. The forwarding options are as follows:
  - Layer 2 point-to-point forwarding to a pseudowire tunnel
  - Multipoint bridge forwarding to a bridge domain entity
  - Local switch-to-switch forwarding between two different interfaces

- Feature commands—In each EFP, the QoS features or parameters can be changed and the ACL can be updated.

Service Instances and Associated EFPs

Configuring a service instance on a Layer 2 port creates a pseudoport or EFP on which you configure EVC features. Each service instance has a unique number per interface, but you can use the same number on different interfaces because service instances on different ports are not related.

An EFP classifies frames from the same physical port to one of the multiple service instances associated with that port, based on user-defined criteria. Each EFP can be associated with different forwarding actions and behavior.

When an EFP is created, the initial state is UP. The state changes to DOWN under the following circumstances:

- The EFP is explicitly shut down by a user.
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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ethernet ring g8032 profile profile-name Creates the Ethernet ring profile and enters Ethernet ring profile configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>timer {guard seconds</td>
</tr>
<tr>
<td>Step 4</td>
<td>non-revertive Specifies a nonrevertive Ethernet ring instance.</td>
</tr>
<tr>
<td></td>
<td>• By default, Ethernet ring instances are revertive.</td>
</tr>
<tr>
<td>Step 5</td>
<td>end Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

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.
Enabling Ethernet Fault Detection for a Service

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ethernet cfm global</td>
</tr>
<tr>
<td>Step 3</td>
<td>link-protection enable</td>
</tr>
<tr>
<td>Step 4</td>
<td>link-protection group management vlan vlan-id</td>
</tr>
<tr>
<td>Step 5</td>
<td>link-protection group group-number pccm vlan vlan-id</td>
</tr>
<tr>
<td>Step 6</td>
<td>ethernet cfm domain domain-name level level-id [direction outward]</td>
</tr>
<tr>
<td>Step 7</td>
<td>service {ma-name</td>
</tr>
<tr>
<td>Step 8</td>
<td>continuity-check [interval time</td>
</tr>
<tr>
<td>Step 9</td>
<td>efd notify g8032</td>
</tr>
<tr>
<td>Step 10</td>
<td>end</td>
</tr>
</tbody>
</table>

Configuring the Ethernet Protection Ring

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ethernet ring g8032 ring-name</td>
</tr>
<tr>
<td>Step 3</td>
<td>port0 interface type number</td>
</tr>
<tr>
<td>Step 4</td>
<td>monitor service instance instance-id</td>
</tr>
<tr>
<td>Step 5</td>
<td>exit</td>
</tr>
<tr>
<td>Step 6</td>
<td>exclusion-list vlan-ids vlan-id</td>
</tr>
</tbody>
</table>
Configuring Topology Change Notification Propagation

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>ethernet tcn-propagation G8032 to {REP</td>
<td>G8032}</td>
</tr>
<tr>
<td></td>
<td>• Source and destination protocols vary by platform and release.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Configuring a Service Instance

To configure a service instance, complete the following steps.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>interface type number</td>
<td>Specifies the interface type and number.</td>
</tr>
<tr>
<td>service instance instance-id ethernet [evc-id]</td>
<td>Creates a service instance (an instance of an EVC) on an interface and enters service instance configuration mode.</td>
</tr>
<tr>
<td>encapsulation dot1q vlan-id [native]</td>
<td>Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.</td>
</tr>
</tbody>
</table>
### Step 5

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridge-domain bridge-id [split-horizon [group group-id]]</td>
<td>Binds the service instance to a bridge domain instance.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>show ethernet ring g8032 status [ring-name] [instance [instance-id]]</td>
</tr>
<tr>
<td>Step 3</td>
<td>show ethernet ring g8032 brief [ring-name] [instance [instance-id]]</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ethernet ring g8032 summary</td>
</tr>
<tr>
<td>Step 5</td>
<td>show ethernet ring g8032 statistics [ring-name] [instance [instance-id]]</td>
</tr>
<tr>
<td>Step 6</td>
<td>show ethernet ring g8032 profile [profile-name]</td>
</tr>
<tr>
<td>Step 7</td>
<td>show ethernet ring g8032 port status interface [type number]</td>
</tr>
<tr>
<td>Step 8</td>
<td>show ethernet ring g8032 configuration [ring-name] instance [instance-id]</td>
</tr>
<tr>
<td>Step 9</td>
<td>show ethernet ring g8032 trace {ctrl [ring-name instance instance-id]</td>
</tr>
<tr>
<td>Step 10</td>
<td>end</td>
</tr>
</tbody>
</table>

### Configuration Examples for Ethernet Ring Protection Switching

#### Example: Configuring Ethernet Ring Protection Switching

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

```plaintext
ethernet ring g8032 profile profile_ABC
timer wrt 1
timer guard 100
timer hold-off 1
ethernet ring g8032 major_ring_ABC
exclusion-list vlan-ids 1000
port0 interface FastEthernet 0/0/0
    monitor service instance 103
port1 interface FastEthernet 0/1/0
```
Example: Enabling Ethernet Fault Detection for a Service

```
eternet cfm domain G8032 level 4
service 8032_service evc 8032-evc vlan 1001 direction down
  continuity-check
  continuity-check interval 3.3ms
  offload sampling 1000
  efd notify g8032
ethernet ring g8032 profile TEST
timer wrt 1
timer guard 100
ethernet ring g8032 open
open-ring
port0 interface GigabitEthernet0/1/3
  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
```

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.

```plaintext
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
```