This chapter describes card and port protection (CPP) for ML-MR-10 card and how to configure CPP using Cisco IOS command line interface (CLI). For information on ML-MR-10 card features, refer ML-Series Card Overview.

This chapter contains the following major sections:

- Understanding CPP
- CPP Switching Parameters
- Error Reporting
- CPP Configuration Example
- Monitoring and Verifying CPP

Contents

- 1 Understanding CPP
- 2 CPP Switching Parameters
- 3 Error Reporting
  - 3.1 CPP Alarms
  - 3.2 Configuring CPP Redundancy
    - 3.2.1 Table 27-1: Commands Related to CPP
- 4 CPP Configuration Example
  - 4.1 Figure 27-1: CPP Configuration Example
  - 4.2 Example 27-1: Creating CPP Protection on Physical Interfaces
  - 4.3 Example 27-2: Create CPP Protection on a port-channel
  - 4.4 Example 27-3: Create CPP Protection on port-channel with LACP
- 5 Monitoring and Verifying CPP
  - 5.1 Example 27-4: show protection detail Command
  - 5.2 Example 27-5: show protection interface Command

Understanding CPP

ML-MR-10 cards can be configured for CPP using a pair of identical ML-MR-10 cards located on the same ONS 15454 chassis and participating in the same IEEE 802.17b-based resilient packet ring (RPR-IEEE). Individual ports can be either CPP protected or unprotected. EtherChannels with or without LACP can be configured for CPP or may remain unprotected. Each EtherChannel can aggregate a maximum of 10 physical members.

For additional information about link aggregation control protocol (LACP) and EtherChannel, refer Configuring Link Aggregation.

In CPP, each Gigabit Ethernet port located at the front of an ML-MR-10 card is protected using the same port number of the protecting ML-MR-10 card. For example, Port 1 of Card A is protected by Port 1 of Card B. The ports must be configured in the same way; that is, their interfaces must have the same attributes, such as, link speed and mode (full or half duplex).

Note: Load balancing across members of the port-channel on the same card is supported irrespective of CPP configuration.

Note: The two cards in the protection group are not verified for configuration consistency.

CPP Switching Parameters

In CPP, two ML-MR-10 cards are configured as peers. A card becomes active or standby under the following conditions:

- When both cards are booted, the first card to come up becomes active and the other card coming up second becomes the standby.
- If both cards come up simultaneously, the card with a lower slot number becomes active and the card with the higher slot number becomes the standby.

If the RPR-IEEE interface goes down or if the front ports do not come up, the active ML-MR-10 card sends a message to the standby card to become active. If the standby card does not become active, both the cards go to pending active state and neither cards perform protection. When an RPR-IEEE interface and a protected front port or port-channel interface comes up for either card, that card becomes active.

Note: The two CPP peer nodes appear as two separate RPR stations in the RPR-IEEE topology.

The active card or port signals the standby card to activate under certain conditions. The following section describes these conditions and the resulting outcome:

- Failed Ethernet link-Switches all the traffic to the peer port on the peer CPP card.
- ML-MR-10 crashes, reloads, or resets-Switches all the protected ports and card to the peer CPP card.
- RPR-IEEE interface is shut down, or all front ports are shut down-Switches all the protected ports and card to the peer CPP card.
- All the port channel members go down-Switches the port channel to the peer port channel interface on the peer CPP card.
- CPP is disabled or unconfigured-Switches all the protected ports and the CPP card state to the peer CPP card.

The standby card becomes active if:

- The active card explicitly requests takeover.
- The active card's periodic heartbeat is missed for two consecutive times.

Note: The active card's heartbeat can be interrupted if it is pulled or if it crashes.

The active card does not recover control of a port from the nonreverting standby card when the front port Ethernet comes back. The active card regains control when the corresponding port fails on the standby card. Similarly, a failed active card cannot recover control from the peer card when the front port Ethernet or RPR-IEEE interface comes up. It becomes active only when the peer card fails or all the front ports of the peer card go down. Unprotected ports are not affected by the state of the protected ports or the CPP card state or any switchover, unless the RPR-IEEE interface goes down. The traffic going through this RPR-IEEE interface then goes down.

Note: The state (active/standby) of the port is independent of the state of the card.

At any given time, a port can be in a transition state other than active or standby. For example:

- A port can temporarily be in a no-control state if it was active but is not yet in the standby mode.
- A port can wait in a no-control state when neither card can claim active control over it.

Note: When a port or port-channel is in standby/down state, the Transmit signal is turned off on the interface so that the peer port can recognize that the link is in standby/down state. However, the link does not go down

for CPP protection with LACP. For CPP standby port-channels, LACP maintains the link in LACP standby state.

Error Reporting

Cisco Transport Controller (CTC) displays the CPP card status: active, standby, or down. When communication between the ML-MR-10 card and the TCC2/TCC2P card goes down and the card fails to send alarms to the TCC2/TCC2P card, error messages are displayed on the Cisco IOS console.

CTC displays the following CPP states to TCC2/TCC2P:

- Card CPP state: Unprotected, Down, Active, or Standby.
- Port CPP state: Unprotected, Down, Active, or Standby.

CPP Alarms

The following alarms are raised in CTC:

- PEER-NORESPONSE: This is a peer-card-not-responding alarm and is raised if an active CPP card does not receive any heartbeat response from its peer card. This occurs if the peer card is not present in the ONS 15454 chassis, or if the peer card is not configured for protection, or if the peer card has reset.
- CPP-INCAPABLE: This is a card-port-protection-incapable alarm and is raised when the ML-MR-10 card or port is unable to provide protection. This condition occurs when the RPR-IEEE interface on the ML-MR-10 card is down, or when the CPP peer slot number is not configured from the Cisco IOS command line interface.

For additional information on these alarms, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 Troubleshooting Guide* or the *Cisco ONS 15454 SDH Troubleshooting Guide* for detailed information.

Configuring CPP Redundancy

Table: Commands Related to CPP describes commands that are related to CPP. For additional information on Cisco IOS commands used in this chapter, refer to the *Cisco IOS Command Reference* publication and the "Command Reference" appendix in the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.

Note: When a node is configured for CPP, the VLANs configured on the CPP nodes must operate with the "service advertisement" option. This enables the remote nodes to send the corresponding VLAN traffic to the CPP card that has the active port.

Table 27-1: Commands Related to CPP

Command	Purpose
`protection group`	Creates a protection group entity. The card then goes to the config-prot mode.
`[no] protection group enable`	Disables a protection group to facilitate troubleshooting or maintenance.
`protection peer slot`	Specifies the slot number of the CPP peer card.
`protection-group`	Adds or deletes a Gigabit Ethernet interface, port-channel and RPR-IEEE interface from the group.

`show protection interface`	Displays protection configuration and status of an interface.
`show protection {detail | group}`	Displays configuration and status of the protection group.

To create a CPP protection group, perform the following procedure, beginning in the global configuration mode. The configuration status is enabled by default.

Step	Command	Purpose
1	`Router(config)# protection group number`	Creates a protection group entity.
2	`Router(config-prot)# protection peer slot slot-number`	Identifies the redundant card.
3	`Router(config-prot)# end`	Exits to privileged EXEC mode.
4	`Router# copy running-config startup-config`	(Optional) Saves configuration changes to NVRAM.

By default, ports are unprotected. Individual ports that are not added in the protection group function because unprotected ports can be used to carry data traffic through Ethernet Flow Point (EFP) configuration. Ensure that protected ports and unprotected ports are configured consistently across CPP peer cards. If protected ports with identical numbers on both CPP peers go to the active state, the card with lower slot number is given precedence.

Note: The configuration of default EFPs does not work on nodes that are configured for CPP. Untagged, double-tagged, and default services will also not work since the "service advertisement" mechanism is not supported for these EFP configuration options.

To disable the group for troubleshooting purposes, enter the following command in the interface configuration mode:

```
Router(config-prot)# no protection group enable
```

For information on other port configuration tasks, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide*.

To assign Ethernet interfaces to the EtherChannel, perform the following procedure, beginning in global configuration mode:

Step	Command	Purpose
1	`Router(config)# interface gigabitethernet number`	Specifies the Gigabit Ethernet interface configuration mode that will be assigned to the EtherChannel.You can assign the Gigabit Ethernet interface to the EtherChannel. Repeat this step for each interface you want to assign.
2	`Router(config-if)# channel-group channel-number`	Assigns a Gigabit Ethernet interfaces to the EtherChannel. The channel number must be the same channel number you assigned to the EtherChannel interface.
3	`Router(config-if)# end`	Exits to privileged EXEC mode.
4	`Router# copy running-config startup-config`	(Optional) Saves configuration changes to NVRAM.

To protect port-channel interfaces using CPP, perform the following procedure:

Step	Command	Purpose
1		

	`Router(config)# interface portchannel number`	Enters the port-channel interface configuration mode.
2	`Router(config-if)# protection-group number`	Configures the port-channel as a CPP protected port.
3	`Router(config-if)# end`	Exits to privileged EXEC mode.
4	`Router# copy running-config startup-config`	(Optional) Saves configuration changes to NVRAM.

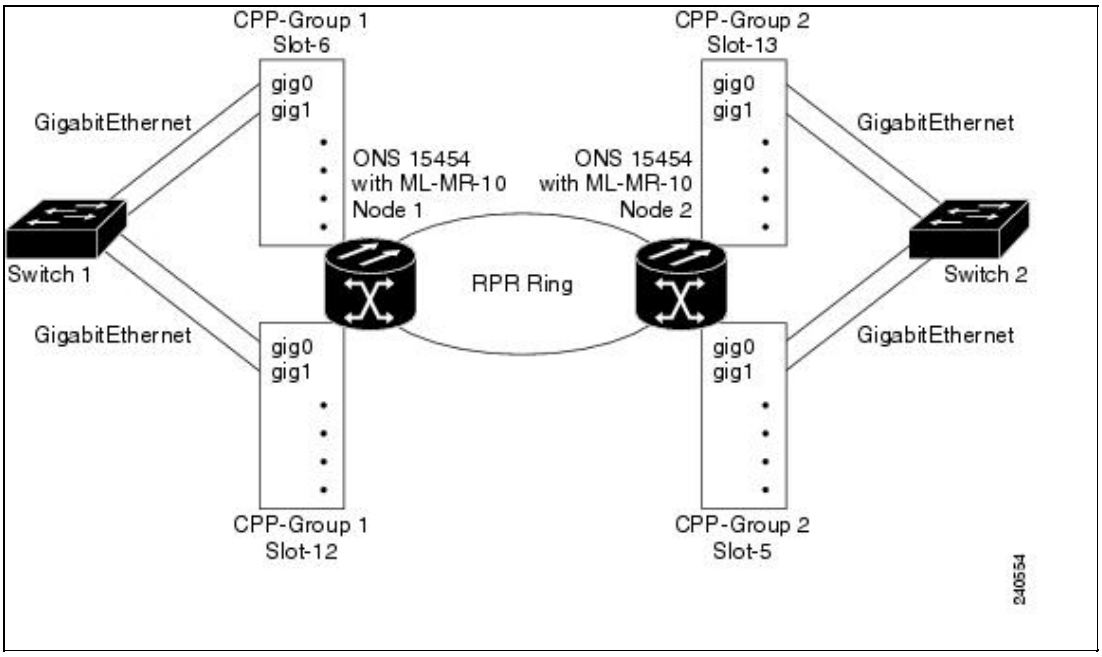
Note: A protection group configuration can similarly be applied to RPR-IEEE and Ethernet ports.

CPP Configuration Example

In Figure 27-1, ML-MR-10 Node 1 (CPP-Group 1 Slot-6) and ML-MR-10 Node 1 (CPP-Group 1 Slot-12) are CPP peers on an ONS 15454.

There can be many such CPP groups on a single node or in an RPR-IEEE ring. However, the CPP peers must be located on a common node. The configuration example in Figure 27-1 illustrates various types of protection. A CPP protection group can be configured on a physical (Gigabit Ethernet) interface, or a logical (port-channel) interface. There can be a combination of interface types on a protection group. The redundancy of each protected interface is maintained during failure, on a peer card with the port numbers of respective (physical/logical) interfaces. Initially, the protected interfaces (that are part of the active card) come up if the physical link's state is up. Based on the status of the link, a port can be in standby or active mode irrespective of the CPP group state.

Figure 27-1: CPP Configuration Example



Note: In any protection type that is configured, RPR-IEEE interface must be part of the protection group.

In the following example, GigabitEthernet0 on CPP-Group 1 Slot-6 protects GigabitEthernet0 on CPP-Group 1 Slot-12 and vice versa. See Figure 27-1. Configuration consistency must be maintained between CPP peer cards. The following configuration is for CPP-Group 1 Slot-6.

Example 27-1: Creating CPP Protection on Physical Interfaces

```
!
protection group 1
    protection peer slot 12
 !
 !
interface GigabitEthernet0
no ip address
no keepalive
duplex auto
speed auto
negotiation auto
protection-group 1
service instance 5 ethernet
encapsulation dot1q 5
bridge-domain 5
!
interface RPR-IEEE0
no ip address
protection-group 1
no rpr-ieee sas
rpr-ieee protection pref jumbo
service instance 5 ethernet
encapsulation dot1q 5
rpr-destination service-advertisement
bridge-domain 5
 !
!
end
```

The following configuration is for CPP-Group 1 Slot-12.

```
protection group 1
    protection peer slot 6
 !
interface GigabitEthernet0
no ip address
no keepalive
duplex auto
speed auto
negotiation auto
protection-group 1
service instance 5 ethernet
encapsulation dot1q 5
bridge-domain 5
!
interface RPR-IEEE0
no ip address
protection-group 1
no rpr-ieee sas
rpr-ieee protection pref jumbo
service instance 5 ethernet
encapsulation dot1q 5
rpr-destination service-advertisement
bridge-domain 5
!
!
end
```

In the following example, port-channel 5 on CPP-Group 1 Slot-6 protects port-channel 5 on CPP-Group 1 Slot-12 and vice versa. See Figure 27-1. Ensure that configuration consistency is maintained between CPP

peer cards. The following configuration is for CPP-Group 1 Slot-6.

Example 27-2: Create CPP Protection on a port-channel

```
!
protection group 1
    protection peer slot 12
 !
 !
 interface Port-channel5
no ip address
no negotiation auto
protection-group 1
load-balance src-dst-mac
hold-queue 0 in
service instance 5 ethernet
encapsulation dot1q 5
bridge-domain 5
 !
service instance 6 ethernet
encapsulation dot1q 6
bridge-domain 6
 !
!
interface GigabitEthernet0
no ip address
no keepalive
duplex auto
speed auto
negotiation auto
channel-group 5
!
interface GigabitEthernet1
no ip address
no keepalive
duplex auto
speed auto
negotiation auto
channel-group 5
!
interface RPR-IEEE0
no ip address
protection-group 1
no rpr-ieee sas
rpr-ieee protection pref jumbo
service instance 5 ethernet
encapsulation dot1q 5
rpr-destination service-advertisement
bridge-domain 5
 !
service instance 6 ethernet
encapsulation dot1q 6
rpr-destination service-advertisement
bridge-domain 6
 !
!
end
```

The following configuration is for CPP-Group 1 Slot-12.

```
!
protection group 1
    protection peer slot 6
```

```
 !
 !
 interface Port-channel5
no ip address
no negotiation auto
protection-group 1
load-balance src-dst-mac
hold-queue 0 in
service instance 5 ethernet
encapsulation dot1q 5
bridge-domain 5
 !
service instance 6 ethernet
encapsulation dot1q 6
bridge-domain 6
 !
 !
interface GigabitEthernet0
no ip address
no keepalive
duplex auto
speed auto
negotiation auto
channel-group 5
!
interface GigabitEthernet1
no ip address
no keepalive
duplex auto
speed auto
negotiation auto
channel-group 5
!
interface RPR-IEEE0
no ip address
protection-group 1
no rpr-ieee sas
rpr-ieee protection pref jumbo
service instance 5 ethernet
encapsulation dot1q 5
rpr-destination service-advertisement
bridge-domain 5
 !
 service instance 6 ethernet
encapsulation dot1q 6
rpr-destination service-advertisement
bridge-domain 6
 !
!
end
```

The configuration of CPP protection on a port-channel with LACP is same as the configuration shown in Example 27-2. The only difference is that the configuration of member Gigabit Ethernet interfaces, as shown in the following example.

For more information on LACP configuration, refer Chapter 10, "Configuring Link Aggregation."

Example 27-3: Create CPP Protection on port-channel with LACP

```
!
interface GigabitEthernet0
no ip address
```

```
no keepalive
duplex auto
speed auto
negotiation auto
channel-group 5 mode active
!
interface GigabitEthernet1
no ip address
no keepalive
duplex auto
speed auto
negotiation auto
channel-group 5 mode active
!
end
```

Monitoring and Verifying CPP

After CPP is configured, you can monitor and verify the card state and the CPP interface states of the current protection group using the **show protection detail** command.

Note: When a failure occurs and the card switches to its peer CPP card, a drop in traffic is observed on the RPR-IEEE if it is oversubscribed.

Example 27-4: show protection detail Command

```
Router# show protection detail
Protection Group: 1
====================
Peer Slot Number     : 12
Group State          : Active
Group FSM State      : Active (Group is Active)
Peer                 : Present
RPR0 interface       : UP

Interface            State
---------            -------
Port-channel5         Active
Router#
```

The following example shows how you can verify the state of the physical interface.

Example 27-5: show protection interface Command

```
Router# show protection interface port-channel 5
Interface Port-channel5:
==========================
Group          : 1
Port State     : Active
Port FSM State : Active (Port is Active)
LACP not configured

MEMBER INTERFACE    LINK FORCED DOWN     LINK STATUS
-------------------------------------------------------
GigabitEthernet0      No                    UP
GigabitEthernet1      No                    UP
GigabitEthernet2      No                    UP
GigabitEthernet3      No                    UP
```

Whenever there is a change in the state of the protection group or port, a message is logged in the Cisco IOS console indicating the new state.

For additional information on CPP alarms, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 Troubleshooting Guide.*