Card Protection for T1 or E1

The card protection feature is supported on the following interface module:

Table 1: Supported Interface Module

Interface Module	Part Number
48-port T1/E1 Interface module	• NCS4200-48T1E1-CE

In this feature, the interface module bay is protected by another interface module of the same type.

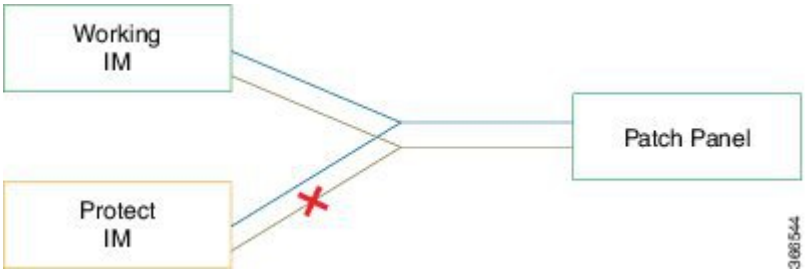
Card Protection

The Card Protection feature is required to protect traffic flow either when an interface module is out of service, when the software fails or a hardware component has issues. Because card protection is supported only on redundant interface modules, traffic is switched to the protect interface module when the active interface module does not respond, and vice-versa.

Note This feature does not require any change in the patch panel of the interface modules.

In card protection, a Y Cable is used to multiplex the signal from the patch panel to both the ports of active and protect interface modules. Both ports receive the signal, but only the active interface module transmits the signal from its port.

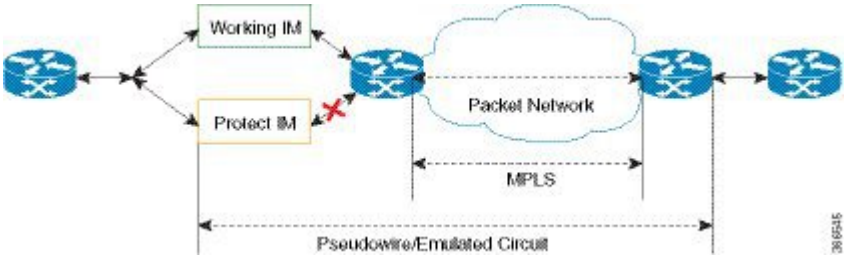
Figure 1: Y Cable



To support the Card Protection feature, the configuration on the active and protect interface module must be same. To achieve this, a virtual interface module is created with the same interface module type as the active interface module. A virtual controller is also created, which broadcasts the configuration to both the interface modules. The configuration on the physical controllers is then blocked and you can make configuration changes only on the virtual controller. The user configuration can only be performed on the virtual controller.

The virtual controller supports CEM level configuration and all other configurations. These configurations are blocked on physical controllers.

Figure 2: Card Protection Topology



Note DS3 (T3) channelized into T1 and E3 channelized into E1s are supported in card protection. For more information on configuration, see the *Configuring the Controller of Channelized T3/T1 Interfaces* section.

Y Cable

In card protection, a Y cable is used to multiplex the signal from the patch panel to both the ports of active and standby interface modules. Both the active and protect ports receive the signal, but only the active port transmits the signal from its port. Protect port transmitter is disabled.

Card Protection Switchover

The following table shows the card protection switchover trigger and time to complete the switchover between the working and protect interface module.

Trigger	Time
Interface Module Reload with CLI OIR	Less than 50 millisecond

Trigger	Time
Non-responsive Interface Module Process (interface module reloads on its own, the reload is initiated due to software error)	100 millisecond to 200 millisecond
Interface Module shuts down due to high temperature	Less than 50 millisecond
Interface Module shuts down using CLI	Less than 50 millisecond
Interface Module stops using CLI	Less than 50 millisecond
Serializer/Deserializer (SerDes) Failures	250 millisecond to 1 second
Alarm Based Switchover	Based on Hold Over Time or Soak Time
Card Protection Commands	20 millisecond to 30 millisecond
Non-responsive Interface Module Process (interface module reloads on its own, the reload is initiated due to software error)	200 millisecond to 1 second
Card Physical Jackout	200 millisecond to 1 second

Alarm Based Switchover

Alarm based switchover is only applicable for Loss Of Signal (LOS) alarm. Switchover happens only when the number of ports with LOS alarm in working interface module is greater than that on the protect interface module.

Each card protection group maintains a weight for each working and protect interface module. This weight is updated when the LOS alarms are asserted or cleared. The switchover happens only if the weight of working interface module and protect interface module stays same for a certain amount of time called soak time.

When there is any issue with the Patch Panel, both working interface module and protect interface module have the same number of LOS alarms (weights are same). Hence, switchover does not happen.

Guidelines on Alarm Based Switchover Scenarios

Considerations for Hold-Off Timer

- With card-protection where Y-cable is used for connecting the protected cards, if Signal Failure (SF) or Signal Degrade (SD) is observed on any of the ports of these protected cards, LOS alarms will be raised on those respective ports. In rare scenarios, these SF/SD notifications across the ports could vary in duration for reporting the LOS alarms due to environment conditions. Hence, to avoid multiple switching between the protected IMs in these scenarios, hold-off timer is introduced to hold the switchover notification till the LOS alarm notification is synchronized on both the IMs.
- Hold-ff timer can be configured using the **hold-off timer** *seconds* CLI command. By Default, (and recommended value for) the hold-off timer value is enabled for 5 seconds.
- When LOS alarms are detected on the ports of the protected IMs, the number of alarm occurrence is compared between the active and standby IM. If the active card has more LOS Alarms, then the hold-off timer gets initiated. After the hold-off timer expiry (5 sec in default case), a protection switch will be triggered to the card having lesser number of alarm notifications.

- If the hold-off timer is set to zero, then the switchover is triggered immediately when the weightage of alarm occurrence in active is more than the standby. Note that in this scenario, it could also lead to multiple protection switching between the IMs till the LOS alarms are settled on all the failed ports of both the IMs.

Considerations for Router Bring up or IM OIR

- During the router bring up or reboot or with Reboot and IM Online Insertion and Removal (OIR), once the IMs are online, there will be alarms flooded to software for all the ports from both the active and standby cards.
- NO operational events or switchover events to be performed during this time, and to allow the alarms on both the IM to be settled. (The approximate recommended duration is 1 minute).

Restrictions

- Card physical jack out convergence time for card protection switchover is more than 50 milliseconds.
- The time taken to restart the interface module due to any software error is more than 50 milliseconds.
- Alarm toggle on active or backup card causes at least one card protection switch.
- When BERT is started from the virtual controllers, the syslog displays the physical controllers instead of the virtual controller port.

Supported Features on Interface Module

The supported features are:

- Switching Mode
  - Non-revertive mode
  - Revertive mode
- Alarm Based Switchover
- SerDes Based Switchover
- Adaptive Clock Recovery (ACR) on virtual CEM
- Differential Clock Recovery (DCR) on virtual CEM
- Maintenance Commands
  - Lockout
  - Force
  - Manual

Note All controller configurations are performed on the virtual controller.

You can create card protection with one slot (either primary or backup) and the remaining slots can be added later.

How to Configure Card Protection for T1 or E1

Configuring T1/E1 Card Protection

Configuring Card Protection Group:

```
enable
configure terminal
card type t1 0 2
card type t1 0 1
card-protection [1-16]
primary slot 0 bay 1
backup slot 0 bay 2
end
```

Note The card protection number 1 to 16 refers to CPGN.

Configuring Virtual Card and Virtual Controller:

When card protection group is configured, it creates virtual card for card protection object, denoted by 8/x/port. Slot 8 is a fixed slot number for all card protection created virtual card. Bay number 'x' for virtual card is x =CPGN -1 = 15. Virtual controllers can be configured from 8/15/0 to 8/15/47.

Physical Card Configuration:

- No configuration is required for traffic.

Virtual Card Configuration:

- Configures CEM on virtual controller (8/x/port).
- Configures xconnect and local connect on CEM interface.

```
enable
configure terminal
controller t1 8/15/0
cem 0 unframed
interface cem 8/15/0
cem 0
xconnect 10.1.1.1 212 encasulation mpls
end
```

```
enable
configure terminal
controller t1 8/15/11
cem 0 unframed
```

```
interface cem 8/15/11
cem 0
connect testLC cem 8/15/0 0 cem 8/15/11 0
end
```

Note To un-configure a CEM group under a virtual controller, first perform shutdown of the virtual controller and then un-configure the CEM group.

Configuring Revertive Mode

To configure revertive mode:

```
enable
configure terminal
card-protection 4
primary slot 0 bay 0
backup slot 0 bay 5
end
card-protection 4
revertive time [30-720]
end
```

Note The revertive time ranges from 30 to 720 seconds.

Verification of T1/E1 Card Protection Configuration

Use **show card-protection** command to verify card protection group configuration.

```
#show card-protection 2 detail
Working(0/1:A900-IMA48T-C NCS4200-48T1E1-CE):
    Number of LOS Alarms:7
    ok,Active
    1:1,  Revertive

    Protect(0/2:A900-IMA48T-C NCS4200-48T1E1-CE):
    Number of LOS Alarms:7
    ok,Inactive
    1:1,  Revertive

Revert Timer : (Not Started)
Last switchover reason :None
```

Use **show xconnect all** command to verify xconnect configuration.

```
#show xconnect all | I CE8/15/
UP   pri   ac CE8/15/0:0(SATOP T1)        UP mpls 10.1.1.1:212             UP
#
```

```
#show xconnect all | i CE8/15/
72       testLC         CE8/15/11 SAT1 0        CE8/15/12 SAT1 0             UP
#
```

Configuring Maintenance Commands

To configure maintenance commands:

```
enable
configure terminal
card-protection 4
primary slot 0 bay 0
backup slot 0 bay 5
end
card-protection 4
card-protection [manual {backup|primary} | force {backup|primary} | lockout]
end
```

Note Maintenance commands are not synced in the standby environment. After Redundancy Force Switchover (SSO), maintenance commands must be executed again on the new active environment.

Priority Table

The following table shows the priority of the actions:

Priority	Configurations
1	Lockout
2	Force
3	Alarm or Card Failure
4	Manual Switch
5	Revert

Associated Commands

The following table shows the commands for the IM configuration:

Command	Link
Card Protection Creation Commands: **card-protection** *CPGN* **card-protection** {*primary* | *backup*} **card-protection** *revertive time* **Card Protection Maintenance Commands**: **card-protection** *CPGN* [**manual** {*primary* | *backup*} | **force** {*primary* | *backup*} | **lockout**]	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c1.html#wp1208639895
show card-protection CPGN detail	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-s2.html#wp1628614402