Router Hardware Management Guide for Cisco 8000 Series Routers, Cisco IOS XR Releases

Cisco 8000 Series Routers
Updated September 11, 2026

Topics included

1 What's changed in this book.....5

Whats changed in this book.....6

2 Hardware modules and compatibility.....7

Compatibility mode for various NPU types.....8

Guidelines for NPU compatibility mode.....9

Restrictions for NPU compatibility mode.....11

Configure NPU compatibility mode.....11

MPA reload.....13

Configure mode 25.....13

Guidelines for using Cisco SFP28 optical modules in the 88-LC1-48Y8H-EM line card.....14

Online Insertion and Removal for optical modules.....16

3 RP redundancy and switchover.....19

Establish RP redundancy.....20

Determine the active RP in a redundant pair.....21

Automatic RP switchover.....22

RP redundancy during RP reload.....22

Manual switchover.....22

Communicate with a standby RP.....24

Summary of redundancy commands.....24

4 Breakout.....25

Breakout mode.....26

Configuration guidelines and restrictions for the breakout mode.....26

Configure the breakout on a port.....26

Remove the breakout configuration.....28

Partial breakout for 400G optics on Cisco 8010 Series routers.....28

Benefits of partial breakout on the Cisco 8011-32Y8L2H2FH router.....29

Partial breakout supported QSFP-DD optics.....29

Partial breakout examples for 400G optics.....30

Partial breakout lane allocation for QSFP-DD modules.....31

5 Power management.....33

NPU power optimization.....34

Configuration guidelines for NPU power optimization.....35

Restrictions for NPU power mode.....36

Configure NPU power mode....36
Dynamic power management....39
Configuration guidelines and restrictions for dynamic power management....40
Power allocation to empty card slot....41
Low-power condition....43
Power allocation to optics....44
Power allocation to fixed-port routers....46
Disable dynamic power management....49
Power redundancy protection....50
Guidelines and restrictions for power redundancy protection....53
Configure single fault protection....53
Configure dual fault protection....55
On-demand transfer of redundant power modules to power reservation pool....57
Ability to set maximum power limit for the router....63

6 Fault detection, recovery, and diagnostics....65
Fabric link management for uncorrectable errors....66
How the router monitors FEC fabric links....67
FEC fabric link system log messages....68
Verify the FEC links....68
Disable fabric link management for uncorrectable errors....69
Fault recovery handling....70
Configure fault recovery attempts....72
Periodic syslog messages for shutdowns due to fault-recovery failures....74
Limitations and restrictions for periodic shutdown syslog messages....75
Machine check error notifications....76
Restrictions for MCE major errors....77
View error details in the Cisco Feature Navigator error messages tool....78
View error details in the MCE log file....78

7 Storage media sanitization....79
Storage media sanitization....80
Secure erase of router SSD data....80
Restriction for secure erase functionality....81
Perform secure erase on a router....82
Storage media sanitization....82
Exclude Sensitive Information in Show Running Configurations Output....83
Sanitize strings....85
Sanitize usernames....85
Sanitize passwords....86
Sanitize comments....87
Sanitize IP addresses....88

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

1 What's changed in this book

Topics:

- Whats changed in this book

This cumulative guide provides a single, continuously updated version that includes all the latest IOS XR features and release updates. It simplifies your experience by letting you bookmark one link and access the complete guide, instead of navigating through multiple release-specific versions.

Whats changed in this book

This cumulative guide provides a single, continuously updated version that includes all the latest IOS XR features and release updates. It simplifies your experience by letting you bookmark one link and access the complete guide, instead of navigating through multiple release-specific versions.

Specific changes or updates tied to individual releases are clearly called out within the relevant sections. For a list of features introduced in a specific release, refer to the Release Notes or the IOS XR Feature Finder.

The table lists the release numbers for which this document has been updated since its initial publication.

Table 1: Changes to this document

Date	Summary
July 2026	First published for Release 26.2.1
September 2026	Republished for Release 26.3.1.

2 Hardware modules and compatibility

Topics:

- Compatibility mode for various NPU types
- MPA reload
- Configure mode 25
- Online Insertion and Removal for optical modules

Describes the operational behavior of hardware modules on Cisco 8000 Series Routers, including Modular Port Adapter reload, online insertion and removal guidelines for optics on Cisco 8000 Series Routers, and compatibility behavior for line cards based on different NPU types.

This chapter describes the hardware modules supported on Cisco 8000 Series Routers and the compatibility behavior between line cards that use different Network Processing Unit (NPU) types.

Compatibility mode for various NPU types

Explains the compatibility mode that allows line cards based on different NPU types to coexist on the same Cisco 8000 series router, and details the resulting boot and operational behavior for each scenario.

Compatibility mode for NPU types is a functionality that:

- allows you to configure the operational mode of line cards within a router, and
- enables interoperability and performance optimization when mixing different generations of NPU-based hardware.

Table 2: Feature history table

Feature Name	Release Information	Description
Configure Compatibility Mode for P200-based Line Cards	Release 25.4.1	You can now configure the compatibility settings for line cards installed in a router to operate in P200 mode. When P200 mode is enabled, only F100-based Fabric Cards (FCs) and P200-based line cards are supported. To enable the P200 NPU mode, use the **hw-module profile npu-compatibility** command.
Optimizing NPU Mode Compatibility for Route Processor Upgrades	Release 24.1.1	When installing Route Processor (RP) cards from different NPU modes or NPU families, the system prioritizes newer generations over older generations. Upgrading to a newer RP, like the 8800-RP2, maintains performance by allowing the use of the Q200 NPU mode without needing to revert to Q100 NPU mode. You can switch to a different NPU mode by using the **hw-module profile npu-compatibility** command.
Configure Compatibility Mode for Q100 and Q200-based Line Cards	Release 7.7.1	You can now configure the compatibility behavior of line cards to operate in Q100 mode (default behavior) or in Q200 mode when you have a mix of Q100-based line cards and Q200-based line cards that are installed in a router. In earlier releases, in a mixed mode combination, if multiple generations of line cards were installed on a distributed chassis, the second-generation line cards interoperated with the first-generation line cards. As as result, the NPUs to set lower resource limits for the newer generation line cards to ensure backward compatibility. The router couldn't fully use the improved scale, higher capacity, and enhanced features of the newer generation line cards. This compatibility feature now enables you to select if you want the line cards to operate in Q100 or Q200 NPU mode. The **hw-module profile npu-compatibility** command is introduced for this feature.

This table details the old and the new behavior when a mix of line cards from different NPUs is installed on a router.

Scenario	If..	Then..	Example
Old behavior	you install a mix of Q100-based line cards and Q200-based line cards	the Q200-based line cards operate in a scaled-down (Q100) mode by default.	If a router has a Q100 NPU-based line card and you add a line card from the Q200 NPU-based line card, the Q200 NPU line card operates in a scaled down mode to work with the Q100 line cards.
New behavior	you want line cards to operate in Q100 (default behavior), Q200, or P100 mode	you can select the mode.	If you select Q200 mode, the router boots only the Q200-based line cards and gracefully shuts down the Q100-based line cards.

FAQs about the compatibility modes for various NPU types

- **Can the line cards still be used in scaled down mode, like in the previous scenario?**

  Yes, you can still switch to the previous implementation, if you may, to the scaled down mode.

- **What all ASICs can participate in the compatibility mode implementation?**

  P200, P100, Q200, Q100.

- **Is there any default ASIC set by the system?**

  The ASIC default is based on the Fabric Cards (FCs) and route processor cards used in a distributed chassis. However, you can choose to change the ASIC mode to Q200, Q100, P100, or P200.

- **Do I need to reboot the router after implementing a new NPU mode?**

  Yes, reboot the router for the new NPU mode to take effect.

- **What defines an NPU mode?**

  The Route Processor determines NPU mode (RP) and the Fabric Card (FC). During the router boot-up process, it initially identifies the RP and the FC, setting the corresponding NPU mode regardless of the line cards present in the router.

Guidelines for NPU compatibility mode

Lists the guidelines that apply when you configure line cards from different ASIC families on a Cisco 8000 series router, including default behaviors, reload requirements, and the line cards that support each compatibility mode.

These guidelines apply when you configure the line cards from different ASIC families.

Line card behavior

- By default, a mix of Q100 and Q200 line cards results in the Q200 line cards operating in Q100 (scaled-down) mode. Configuring Q100 mode results in the same (default) behavior. Similarly, a mix of P100 and Q200 line cards results in the Q200 line cards operating in P100 (scaled-down) mode. Configuring P100 mode results in the same (default) behavior.
- Reboot the router for the compatibility mode to take effect. If the system detects a non-compatible line card, it shuts down that line card. For example, in Q200 mode, the router boots only the Q200-based line cards and gracefully shuts down the Q100-based line cards.

- If you have various line cards installed from different NPU families, the newer generation line cards take precedence over an older generation line card. The precedence followed by the system is: P200 > P100 > Q200 > Q100.

Optimizing line card performance

To use the improved scale, higher capacity, and feature-rich capabilities of the Q200-based line cards, use the **hw-module profile npu-compatibility** command and set it to operate in the Q200 mode. Else, the Q200-based line cards scale down to the Q100 mode, which is the default behavior. The same behavior applies to the P100-based line cards.

Fabric card behavior

- 8800-RP Route Processor Card - if the router boots up with an 8800-RP route processor card without any fabric card, then the default mode is set to Q100.
- 8800-RP2 Route Processor Card - if the router boots up with a 8800-RP2 route processor card without any fabric card, then the router sets the default mode to P100. If you insert a Q200 fabric card, then router reload is required.
- Swapping Fabric Cards - if the router initially boots with Q200 fabric cards and you later replace them with F100 fabric cards, a router reload is necessary.

Route processor behavior

- For 8800-RP, the default NPU mode is Q100. For 8800-RP2, the default NPU mode is Q200.
- A newer generation Route Processor (RP) card takes precedence over an older generation RP card when installed from different NPU modes. The precedence followed by the system is: P200 > P100 > Q200 > Q100.
- If you have Q200-based line cards and an older generation RP card (8800-RP) installed on your router, the router boots with Q100 ASIC mode for the line cards. However, you can change the ASIC mode from Q100 to Q200 by using the **hw-module profile npu-compatibility** command. Setting the ASIC mode to a newer generation ASIC allows you to use their improved scale, higher capacity, and feature-rich capabilities when you replace your RPs with a newer generation RP.

  For instance, if your router is equipped with an 8800-RP route processor card set to ASIC mode as Q200, upgrading to an 8800-RP2 RP card won't require changing the ASIC mode from Q100 to Q200.

Compatibility mode support on line cards

This table lists the Q100, Q200, P100-based, and P200 line cards that support the compatibility mode:

ASIC Family	Line Card
Q100-based line cards	8800-LC-48H
	8800-LC-36FH
Q200-based line cards	88-LC0-34H14FH
	88-LC0-36FH
	88-LC0-36FH-M
P100-based line cards	88-LC1-36EH
	88-LC1-12TH24FH-E
	88-LC1-52Y8H-EM

Restrictions for NPU compatibility mode

Lists the restrictions that apply when you configure line cards from different ASIC families, including unsupported platforms, unsupported ASIC, and route processor combinations.

Restrictions for compatibility mode configuration

These restrictions apply when you configure the line cards from different ASIC families:

- The **hw-module profile npu-compatibility** command isn't configurable on the Cisco 8200 Series fixed router and the Cisco 8608 router.
- Q100-based ASIC is not supported with 8800-RP2-S.
- P200-based ASIC.

Configure NPU compatibility mode

Describes how to configure the NPU compatibility mode for line cards on a Cisco 8000 series router, so that line cards from different NPU families coexist in the selected ASIC mode.

To configure a router for handling line cards of different NPU-based line cards, use the **hw-module profile npu-compatibility** command. To go back to the default mode, use the **no** form of this command.

These are the options available in command and their descriptions:

npu-compatibility	Allows you to make a router compatible with a NPU family.
mode-name	Allows you to set the mode, such as Q100, Q200, P100 , or P200.

Procedure

1. Enter global configuration mode.

   Example

   ```
   Router# configure
   ```

2. Use the hw-module profile npu-compatibility command to define the operational NPU mode for the router. In this example, the NPU compatibility mode is set to Q200.

   Example

   ```
   Router(config)#hw-module profile npu-compatibility q200
   Tue Dec 7 15:06:53.697 UTC
   ```

3. Save the changes.

   Example

   ```
   Chassis mode will be activated after a manual reload of chassis/all line cards
   Router:ios(config)#commit
   ```

4. When prompted, reload the router.

Example

```
Tue Dec 7 15:06:54.646 UTC
LC/0/1/CPU0:Dec 7 15:06:54.796 UTC: npu_drvr292:
%FABRIC-NPU_DRVR-3-HW_MODULE_PROFILE_NPU_COMPATIBILITY_CHASSIS_CFG_CHANGED :
 Please reload
chassis for the configuration to take effect
end
```

5. Verify the running configuration and the software version. The **Version** field defines the software version.

Example

```
Router# show ver
Mon Jun 27 19:25:52.947 UTC
Cisco IOS XR Software, Version 7.7.1.27I LNT
Copyright (c) 2013-2022 by Cisco Systems, Inc.

Build Information:
 Built By     : ingunawa
 Built On     : Wed Jun 01 23:50:09 UTC 2022
 Build Host   : iox-ucs-060
 Workspace    : /auto/iox-ucs-060-san1/prod/7.7.1.27I.SIT_IMAGE/8000/ws
 Version      : 7.7.1.27I
 Label        : 7.7.1.27I

cisco 8000 (VXR)
cisco 8808 (VXR) processor with 32GB of memory
ios uptime is 3 minutes
Cisco 8808 8-slot Chassis

Router#

Router# conf
Mon Jun 27 19:24:40.621
Router(config)#hw-module profile npu-compatibility ?

  P100  Use P100 for Chassis mode
  Q100  Use Q100 for Chassis mode
  Q200  Use Q200 for Chassis mode
```

6. Verify the compatibility matrix on the router.

Example

```
Router# show hw-module profile npu-compatibility matrix
Wed Nov 17 02:00:28.652 UTC
Node              Card Type                NPU Type
-----------------------------------------------------
0/0/CPU0          88-LC0-36FH              Q200
0/1/CPU0          88-LC1-36EH              P100
0/2/CPU0          88-LC1-36EH              P100
0/3/CPU0          88-LC1-36EH              P100

             Compatibility       Compatibility       Compatibility
Compatibility       Compatibility       Compatibility       Compatibility
NPU Type   Mode Q100            Mode Q200            Mode G100
Mode P100            Mode A100            Mode K100            Mode F100
-----------------------------------------------------------------------
```

```
Q100        Compatible          Not Compatible      Not Compatible      Not
Compatible      Not Compatible      Not Compatible      Not Compatible
Q200        Compatible          Compatible          Not Compatible      Not
Compatible      Not Compatible      Not Compatible      Not Compatible
G100        Not Compatible      Compatible          Compatible          Not
Compatible      Not Compatible      Not Compatible      Not Compatible
P100        Not Compatible      Not Compatible      Not Compatible      Not
Compatible      Not Compatible      Not Compatible      Not Compatible
A100        Not Compatible      Not Compatible      Not Compatible      Not
Compatible      Not Compatible      Not Compatible      Not Compatible
K100        Not Compatible      Not Compatible      Not Compatible      Not
Compatible      Not Compatible      Not Compatible      Not Compatible
F100        Not Compatible      Not Compatible      Not Compatible      Not
Compatible      Not Compatible      Not Compatible      Not Compatible
Default mode : P100
Router#
```

MPA reload

Describes how the data path power-on timer manages Modular Port Adapter initialization on Cisco 8000 series routers and triggers an automatic reload when an MPA does not come up within 20 minutes.

A Modular Port Adapter (MPA) is a hardware component that

- provides flexible and scalable port configurations, and
- is used in networking equipment, such as routers and switches.

A data path power-on timer is used during the power-on sequence of a network device to manage the initialization, stabilization, and diagnostic processes of the data path components. If an MPA card doesn't come up within 20 minutes, the data path power-on timer expires, and the MPA goes for another reload to attempt recovery.

> **Note**
>
> When a router enters an undefined state and disrupts the traffic due to the data path power-on timer expiry (timer associated with a data path has expired), reload the router using the **reload location** command.

Configure mode 25

Provides instructions on how to configure mode 25 in a controlled workflow. Covers prerequisites, execution steps, and result checks needed for successful completion.

To support 25G (SFP28) modules, configure the mode as 25 on the designated port pairings. This configuration activates the primary port for 25G (SFP28) module insertion while disabling the secondary port in each pair.

Procedure

1. Enter the global configuration mode.

Example

```
Router# configure terminal
```

2. Configure **mode 25** using the **hw-module port-range** *start-port end-port* **location** *node-id* **mode 25** command for the desired port pairing. Insert the module into the *start-port* port number of the pair.

   Example

   ```
   Router(config)# hw-module port-range 7 8 location 0/0/CPU0 mode 25
   ```

3. Commit the configuration.

   Example

   ```
   Router(config)# commit
   ```

Verify that the system reflects the intended configuration state.

What to do next

Continue with related procedures as required by your workflow.

Guidelines for using Cisco SFP28 optical modules in the 88-LC1-48Y8H-EM line card

Details key principles for guidelines for using Cisco SFP28 optical modules in the 88-LC1-48Y8H-EM line card that guide safe and consistent operation. Explains applicability, rationale, and expected outcomes for technical users.

Use these guidelines to operate the Cisco SFP28 optical modules in the 88-LC1-48Y8H-EM line card:

- The SFP28 modules can operate in the following SFP ports (top row of the front panel) without any exclusive port-range configuration.
  - Port 6, 9, 12, 15, 18, 21, 24, 27, 34, 37, 40, 43, 46, 49, 52 and 55.
- The SFP28 modules can operate in the following SFP ports (middle row of the front panel) by configuring the **hw-module port-range** *start-port end-port* **location** *node-id* **mode 25** command with the supported port-pairs.
  - Port 7, 10, 13, 16, 19, 22, 25, 28, 35, 38, 41, 44, 47, 50, 53 and 56
- The SFP28 modules are not supported on the following ports (bottom row of the front panel). These ports are disabled when the **port-range** configuration is committed, on a given port-pair
  - Port 8, 11, 14, 17, 20, 23, 26, 29, 36, 39, 42, 45, 48, 51, 54 and 57

Note

Use the following command to configure the **port-range** in order to support the SFP28 modules:

hw-module port-range *start-port end-port* **location** *node-id* **mode 25**

When this command is applied to a supported port pair:

- The *start-port* is enabled for 25/10/1 GbE operations.
- The *end-port* in the pair is disabled.

Supported port pairings on the 88-LC1-48Y8H-EM line card

Provides reference details for supported port pairings on the 88-LC1-48Y8H-EM line card used during configuration and validation. Covers key values, constraints, and supporting technical data for quick lookup.

Cisco SFP28 optical modules are supported on these port pairings of the 88-LC1-48Y8H-EM line card:

Start Port	End Port
7	8
10	11
13	14
16	17
19	20
22	23
25	26
28	29
35	36
38	39
41	42
44	45
47	48
50	51
53	54
56	57

Online Insertion and Removal for optical modules

Provides Online Insertion and Removal (OIR) guidelines for optical modules on the routers, MPA, and line cards.

These guidelines apply for the Online Insertion and Removal (OIR) of the optical modules on these routers, MPA, and line card:

- Cisco 8711-48Z-M router
- Cisco 8712-MOD-M router with 8K-MPA-18Z1D MPA
- Cisco 88-LC1-48Y8H-EM line card
- Cisco 8404-SYS-D with 84-MPA-2H12Z-M MPA

Guidelines for re-inserting optics

- After removing certain Cisco 1G Bidirectional optics, 1G Coarse Wavelength Division Multiplexing (CWDM) optics, or 10G Bidirectional SFP optics, wait for at least 15 minutes before re-inserting the same optics into any SFP port.
- The 15 minute wait time also applies to all third-party 1G and 10G optics, as their behavior is not verified by Cisco.
- This wait time does not apply when installing new or unused optics.

The wait time applies to these optics:

Optics Type	PID
Cisco 1G Bidirectional Optics	• GLC-BX40-DA-I • GLC-BX40-D-I • GLC-BX40-U-I • GLC-BX80-D-I • GLC-BX80-U-I For more details, refer to the Data sheet.
Cisco 1G CWDM Optics	CWDM-SFP-xxxx For more details, refer to the Data sheet.
Cisco 10G Bidirectional Optics	• SFP-10G-BXD-I • SFP-10G-BXU-I • SFP-10G-BX40U-I • SFP-10G-BX40D-I For more details, refer to the Data sheet.
Third-party 1G and 10G optics	NA

Wait time guidelines applicable to Cisco 8711-48Z-M router

- The 48 SFP56 ports are divided into four groups:
  - Group 1: Ports 0-11
  - Group 2: Ports 12-23

  - Group 3: Ports 34-45
  - Group 4: Ports 46-57
- Group 5: Ports 24-33, includes four QSFP56 and six QSFP-DD ports.
- If the same optics are re-inserted on the router within 15 minutes, a brief disruption or link flap may occur on the remaining 11 SFP56 ports of the same group. Other groups remain unaffected.
- Inserting optics into Group-5 ports does not cause any disruptions.

Wait time guidelines applicable to Cisco 8712-MOD-M router with 8K-MPA-18Z1D MPA

- The 19 ports (18 SFP56 + 1 QSFP56-DD) are divided into two groups:
  - Group 1: Ports 0-8
  - Group 2: Ports 9-18
- If the same optics are re-inserted on the router within 15 minutes, a brief disruption or link flap may occur on the remaining ports of the same group. Other groups remain unaffected and ports on other MPAs remain unaffected.
- Inserting optics into QSFP28, QSFP56, or QSFP-DD ports does not cause any link disruptions.

Wait time guidelines applicable to Cisco 88-LC1-48Y8H-EM line card

- 48 ports of SFPs are divided into 3 groups:
  - Group 1: Ports 6, 9, 12, 15, 18, 21, 24, 27, 34, 37, 40, 43, 46, 49, 52, 55.
  - Group 2: Ports 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26, 28, 29.
  - Group 3: Ports 35, 36, 38, 39, 41, 42, 44, 45, 47, 48, 50, 51, 53, 54, 56, 57.
- If the same optics are re-inserted on the line card within 15 minutes, a brief disruption or link flap may occur on the remaining ports of the same group.
- Inserting optics into QSFP28, QSFP56, or QSFP-DD ports does not cause any link disruptions.

Wait time for re-inserting 1G and 10G optics in Cisco 8404-SYS-D with 84-MPA-2H12Z-M MPA

When using the Cisco 8404-SYS-D chassis equipped with the 84-MPA-2H12Z-M MPA, special considerations are required when removing and re-inserting certain 1G and 10G optics. Proper wait times help prevent network disruptions and maintain stable operation, especially when dealing with specific SFP types and third-party optics.

Key Recommendation

After removing any of the following optics from the 84-MPA-2H12Z-M MPA module, you must wait at least 15 minutes before re-inserting the same optic into any SFP port:

> **Note**
>
> No 15-minute wait is required when installing new (unused) optics.

Impact when you insert SFP optic within 15 minutes

If you re-insert the same SFP optic within 15 minutes on the 8404-SYS-D with the 84-MPA-2H12Z-M MPA:

- Same groups: There may be a brief link disruption (link flap) on the other ports within the same group as the port where the optic is inserted.

- Other groups and MPAs: Ports in other groups on the same MPA, or on other MPAs in the same chassis, will not experience any link disruption.

Port Grouping

- The 84-MPA-2H12Z-M MPA has a total of 14 ports (12 SFP + 2 QSFP), divided into two groups:
  - Group 1: Ports 0-7
  - Group 2: Ports 8-13

- QSFP28 Ports: Inserting optics into QSFP28 ports does not cause link disruptions on any ports

3 RP redundancy and switchover

Topics:

- Establish RP redundancy
- Determine the active RP in a redundant pair
- Automatic RP switchover
- RP redundancy during RP reload
- Manual switchover
- Communicate with a standby RP
- Summary of redundancy commands

Outlines route processor redundancy and switchover on the router. Covers how redundancy is established, how the active and standby RPs are identified, automatic and manual switchover, behavior during RP reload, standby communication, and the commands used to manage redundancy.

This chapter describes RP redundancy and switchover commands and issues.

Establish RP redundancy

Describes how to establish route processor redundancy by installing RPs into both RP slots of the chassis, which are configured for redundancy by default and cannot have redundancy disabled.

The router has two slots for RPs that face the front of the chassis:

- RP0
- RP1

Refer to Figure 1: Redundant set of RP installed in slots RP0 and RP1 in a Cisco 8608 8-slot centralized chassis on page 20 and Figure 2: Redundant set of RP installed in slots RP0 and RP1 in a Cisco 8808 8-slot distributed chassis on page 20). RP0 is the slot on the left, facing the front of the chassis, and RP1 is the slot on right.

Figure 1: Redundant set of RP installed in slots RP0 and RP1 in a Cisco 8608 8-slot centralized chassis

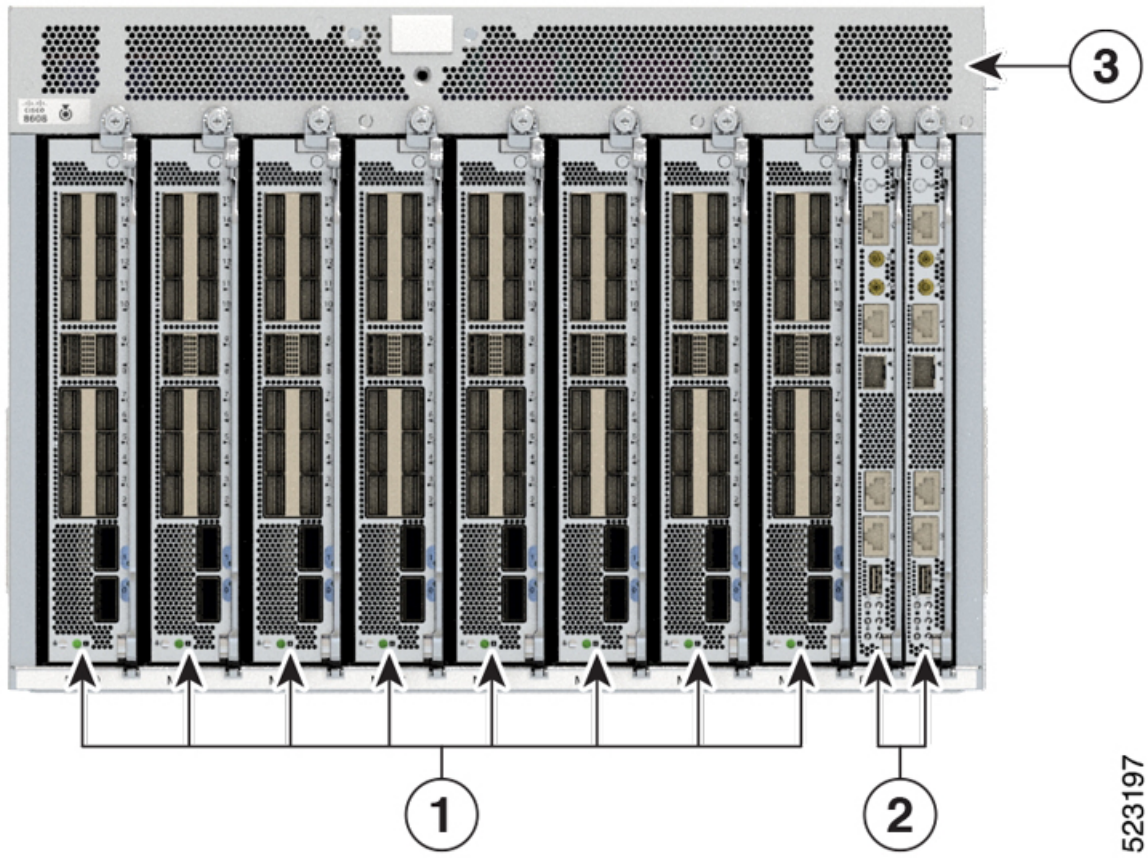
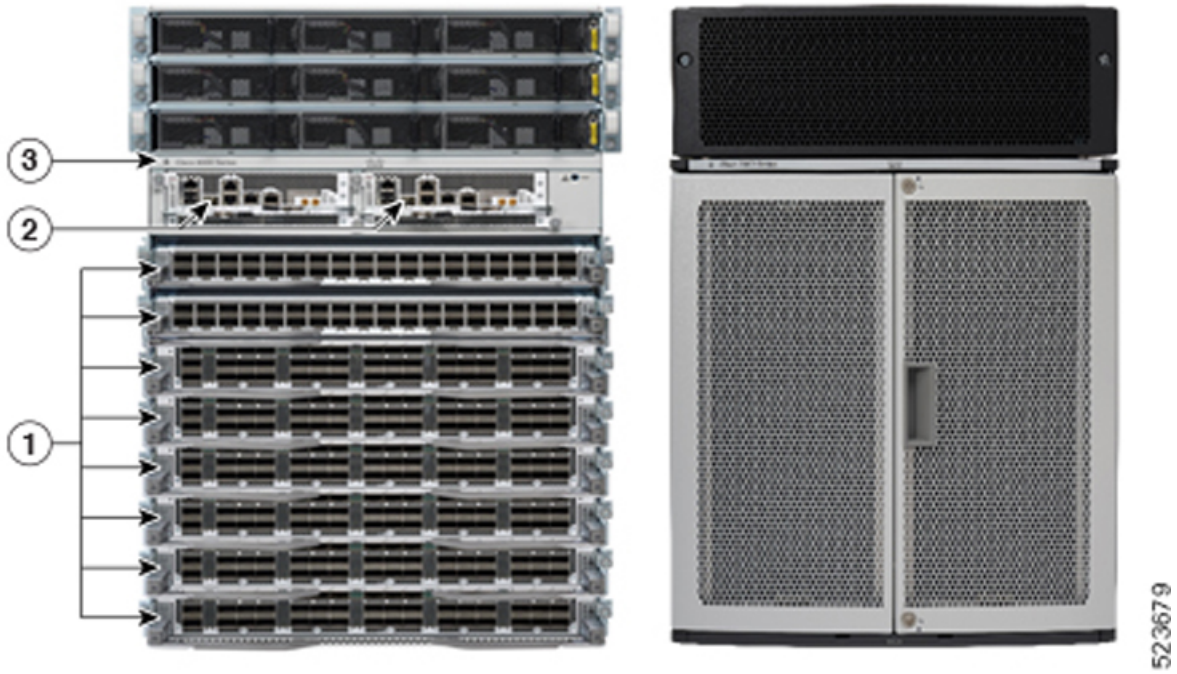


Figure 2: Redundant set of RP installed in slots RP0 and RP1 in a Cisco 8808 8-slot distributed chassis



1	Modular Port Adaptors (MPAs)
2	Route Processors (RPs)
3	Chassis

Active RP

The active RP manages the system and communicates with the user interface.

Standby RP

The standby RP maintains a complete backup of the software and configurations for all cards in the system. If the active RP fails or goes offline for any reason, the standby RP immediately takes control of the system.

Determine the active RP in a redundant pair

Describes how to identify the active route processor in a redundant pair using the green Active LED on the card faceplate.

During system startup, one RP in each redundant pair becomes the active RP. You can identify the active RP in these ways:

- The active RP is identifiable by the green Active LED on the faceplate of the card. When the Active LED turns on, it indicates that the RP is active. When the Active LED turns off, it indicates that the RP is in standby.
- The slot of the active RP is indicated in the CLI prompt. For example:

```
Router#
```

In this example, the prompt indicates that you are communicating with the active RP in slot RP1.

- Use the **showredundancy** command in EXEC mode to display a summary of the active and standby RP status. For example:

```
Router# show redundancy

  This node (0/RP0/CPU0) is in ACTIVE role
  Partner node (0/RP1/CPU0) is in STANDBY role
  Standby node in 0/RP1/CPU0 is ready

  Reload and boot info
  ----------------------
  RP reloaded Fri Apr  9 03:44:28 2004: 16 hours, 51 minutes ago
  This node booted Fri Apr  9 06:19:05 2004: 14 hours, 16 minutes ago
  Last switch-over Fri Apr  9 06:53:18 2004: 13 hours, 42 minutes ago
  Standby node boot Fri Apr  9 06:54:25 2004: 13 hours, 41 minutes ago
  Standby node last not ready Fri Apr  9 20:35:23 2004: 0 minutes ago
  Standby node last ready Fri Apr  9 20:35:23 2004: 0 minutes ago
  There have been 2 switch-overs since reload
```

Automatic RP switchover

Describes how an automatic switchover from the active route processor to the standby occurs when the active RP encounters a serious system error.

Automatic switchover from the active RP to the standby RP occurs only if the active RP encounters a serious system error, such as the loss of a mandatory process or a hardware failure. When an automatic switchover occurs, the RPs respond in these ways:

- If a standby RP is installed and ready for switchover, the standby RP becomes the active RP. The original active RP attempts to reboot.
- If the standby RP is not in the ready state, then both RPs reboot. The first RP to boot successfully adopts the role of active RP.

RP redundancy during RP reload

Describes how the active and standby route processors respond when an operator runs the reload command on an active RP.

The **reload** command causes the active RP to reload the Cisco IOS XR software. When an RP reload occurs, the RPs respond in these ways:

- If a standby RP is installed and ready for switchover, the standby RP becomes the active RP. The original active RP reboots and becomes the standby RP.
- If the standby RP is not in the ready state, then both RPs reboot. The first RP to boot successfully adopts the role of active RP.

Manual switchover

Describes how to force a manual switchover from the active route processor to the standby by running the redundancy switchover command or by reloading the active RP with the reload command.

If a standby RP is installed and ready for switchover, you can perform the switchover by using these commands:

- The **redundancyswitchover** command
- The **reload** command.

Manual switchover using the redundancy switchover command

You can force a manual switchover from the active RP to the standby RP by using the **redundancyswitchover** command.

If a standby RP is installed and ready for switchover, the standby RP becomes the active RP. The original active RP becomes the standby RP. In this example, partial output for a successful redundancy switchover operation is shown:

```
Router# show redundancy

  This node (0/RP0/CPU0) is in ACTIVE role
  Partner node (0/RP1/CPU0) is in STANDBY role
  Standby node in 0/RP1/CPU0 is ready

  Router# redundancy switchover
  Updating Commit Database.  Please wait...[OK]
  Proceed with switchover 0/RP0/CPU0 -> 0/RP1/CPU0? [confirm]
  Initiating switch-over.
  Router#

<Your 'TELNET' connection has terminated>
```

Manual switchover using the reload command

You can force a manual switchover from the active RP to the standby RP by reloading the active RP using the **reload** command. As active RP reboots, the current standby RP becomes active RP, and rebooting RP switches to standby RP.

```
Router# reload
Router#
```

In the earlier example, the Telnet connection is lost when the previously active RP resets. To continue management of the router, you must connect to the newly activated RP as shown in this example:

```
User Access Verification

  Username: xxxxx
  Password: xxxxx
  Last switch-over Sat Apr 15 12:26:47 2009: 1 minute ago

Router#
```

If the standby RP is not in the ready state, the switchover operation is not allowed. In this example, partial output for a failed redundancy switchover attempt is shown:

```
Router# show redundancy

  Redundancy information for node 0/RP1/CPU0:
  ==========================================
  Node 0/RP0/CPU0 is in ACTIVE role
  Partner node (0/RP1/CPU0) is in UNKNOWN role

  Reload and boot info
  ----------------------
  RP reloaded Wed Mar 29 17:22:08 2009: 2 weeks, 2 days, 19 hours, 14 minutes
 ago
  Active node booted Sat Apr 15 12:27:58 2009: 8 minutes ago
```

```
Last switch-over Sat Apr 15 12:35:42 2009: 1 minute ago
There have been 4 switch-overs since reload

Router# redundancy switchover

Switchover disallowed: Standby node is not ready.
```

Communicate with a standby RP

Explains how the active route processor synchronizes system software, settings, and configurations with the standby RP, and how an operator can view standby status messages through the console port without a CLI prompt.

The active RP automatically synchronizes all system software, settings, and configurations with the standby RP.

If you connect to the standby RP through the console port, you can view the status messages for the standby RP. The standby RP does not display a CLI prompt, so you cannot manage the standby card while it is in standby mode.

If you connect to the standby RP through the management Ethernet port, the prompt that appears is for the active RP, and you can manage the router the same as if you had connected through the management Ethernet port on the active RP.

Summary of redundancy commands

Lists the Cisco IOS XR commands that display the redundancy status of route processor cards and the command used to force a manual switchover.

RP redundancy is enabled by default in the Cisco IOS XR software but you can use the commands described in this table to display the redundancy status of the cards or force a manual switchover.

Table 3: RP redundancy commands

Command	Description
showredundancy	Displays the redundancy status of the RP. This command also displays the boot and switch-over history for the RP.
redundancyswitchover	Forces a manual switchover to the standby RP. This command works only if the standby RP is installed and in the "ready" state.
show platform	Displays the status for node, including the redundancy status of the RP cards. In EXEC mode, this command displays status for the nodes assigned to the SDR. In administration EXEC mode, this command displays status for all nodes in the system.

4 Breakout

Topics:

- Breakout mode
- Configuration guidelines and restrictions for the breakout mode
- Configure the breakout on a port
- Remove the breakout configuration
- Partial breakout for 400G optics on Cisco 8010 Series routers

This chapter describes the breakout mode on the router, the guidelines and restrictions that apply to the breakout mode, the tasks for configuring the breakout on a port and removing the breakout configuration, and the partial breakout feature for 400G optics on Cisco 8010 Series routers.

Breakout mode

This topic describes how the router supports transmission of traffic in the breakout mode, which enables a 40 Gigabit Ethernet port to be split into four independent and logical 10 Gigabit Ethernet ports on supported 40G modules.

The breakout mode is a port configuration feature that

- enables the splitting of a 40 Gigabit Ethernet port into four independent logical 10 Gigabit Ethernet ports
- facilitates flexible bandwidth distribution, and
- supports specific 40G module types.

> **Note**
>
> The Cisco 8010 Series Routers do not support this feature. For a list of supported features on the Cisco 8010 Series Routers, see *Compatibility Matrix for Cisco 8010 Series Routers*.

The 4x10 breakout mode is supported on the following types of 40G modules:

- QSFP-4x10-LR-S
- QSFP-40G-SR4

Configuration guidelines and restrictions for the breakout mode

This topic lists the guidelines and restrictions that apply when you configure the breakout mode.

- If you're using a Q100-based Cisco 8200 Series Router and want to set up a 4x10G breakout configuration, you need to use even-numbered ports from 24 to 35. These include ports 24, 26, 28, 30, 32, and 34. Once you do this, the system automatically disables the odd-numbered ports in this range – ports 25, 27, 29, 31, 33, and 35.
- Use the **hw-module port-range** command to set the port range for the breakout configuration in the global configuration.
- To remove the global **hw-module port-range** configuration, you must first remove the **breakout 4x10** configuration under the controller.
- On the Cisco 8812 router, the 88-LC0-34H14FH line card can have only three ports per Interface Group (IFG) when operating in 4x10 GbE or 4x25 GbE breakout configuration mode. This helps prevent the `QOS-DPA_QOSEA-2-TMPORT_PROG_ERROR` issue, which creates partial interfaces during configuration mode.

Configure the breakout on a port

This topic describes how to configure the breakout mode on an optics controller of a port so that the router splits the port into four independent and logical 10 Gigabit Ethernet subports.

Configure the breakout mode on the optics controller of a port to split the port into four 10 Gigabit Ethernet subports.

Procedure

1. Enter global configuration mode.

   Example

```
Router# configure
Fri Oct 11 23:58:47.165 UTC
```

2. Enter optics controller configuration mode for the target port.

   Example

```
Router(config)# controller optics 0/1/0/28
```

3. Configure the 4x10 breakout on the optics controller.

   Example

```
Router(config-Optics)# breakout 4x10
```

4. Commit the configuration and exit the configuration mode.

   Example

```
Router(config-Optics)# commit
Fri Oct 11 23:59:51.261 UTC
RP/0/RP0/CPU0:uut(config-Optics)# end
RP/0/RP0/CPU0:uut#
```

5. Verify the breakout configuration on the optics controller and view the four 10 Gigabit Ethernet subinterfaces created by the breakout.

   Example

```
Router# show running-config controller optics 0/1/0/28
Sat Oct 12 00:11:33.962 UTC
controller Optics0/1/0/28
breakout 4x10
!

Router# show int br location 0/1/CPU0 | i Te
Sat Oct 12 00:11:38.609 UTC
      Te0/1/0/27/0          up         up              ARPA 10000   10000000

      Te0/1/0/27/1          up         up              ARPA 10000   10000000

      Te0/1/0/27/2          up         up              ARPA 10000   10000000

      Te0/1/0/27/3          up         up              ARPA 10000   10000000

      Te0/1/0/28/0          up         up              ARPA 10000   10000000

      Te0/1/0/28/1          up         up              ARPA 10000   10000000

      Te0/1/0/28/2          up         up              ARPA 10000   10000000
```

```
      Te0/1/0/28/3          up          up               ARPA 10000   10000000
```

Remove the breakout configuration

This topic describes how to remove the 4x10 breakout configuration from an optics controller of a port so that the router restores the port to its original 40 Gigabit Ethernet operating mode.

Remove the breakout configuration from the optics controller of a port that was previously configured with the 4x10 breakout mode.

Procedure

1. Enter global configuration mode.

   Example

   ```
   Router# configure
   Sat Oct 12 00:01:38.673 UTC
   ```

2. Enter optics controller configuration mode for the target port.

   Example

   ```
   Router(config)# controller optics 0/1/0/28
   ```

3. Remove the 4x10 breakout configuration from the optics controller.

   Example

   ```
   Router(config-Optics)# no breakout 4x10
   ```

4. Commit the configuration and exit the configuration mode.

   Example

   ```
   Router(config-Optics)# commit
   Sat Oct 12 00:01:55.864 UTC
   RP/0/RP0/CPU0:uut(config-Optics)# end
   ```

Partial breakout for 400G optics on Cisco 8010 Series routers

Explains how the partial breakout feature for 400G optics enables flexible port combinations and maximizes hardware utilization on Cisco 8010 Series routers.

A partial breakout feature is a hardware capability that

- allows a QSFP-DD 4×100GE optic to provide four distinct 100GE electrical lanes
- enables different configurations so that not all lanes must be active or used in a single front-panel port, and
- allows unused lanes to be reallocated to other ports for greater flexibility and improved hardware utilization.

Table 4: Feature History Table

Feature Name	Release Information	Feature Description
Partial breakout for 4×100GE QSFP-DD optics	Release 26.3.1	Introduced in this release on: Fixed Systems (8010 [ASIC: A100])(select variants only*) This feature enables flexible port combinations and maximizes hardware usage on the Cisco 8011-32Y8L2H2FH router by allowing a 4x100GE optic to be used as a 1x100GE, 2x100GE, or 3x100GE so that unused SerDes (Serializer/Deserializer) lanes can be reallocated to other ports. *This feature is supported only on the Cisco 8011-32Y8L2H2FH router.

Partial breakout for 4×100GE QSFP-DD optics on Cisco 8010 Series routers

Starting with Cisco IOS XR Release 26.2.1, partial breakout for QSFP-DD 4x100GE optics provides port-level flexibility and improves hardware utilization on the Cisco 8011-32Y8L2H2FH router, which is equipped with *H100 (Helium-100) physical layer (PHY) devices*[1].

Benefits of partial breakout on the Cisco 8011-32Y8L2H2FH router

Outlines the benefits for partial breakout on the Cisco 8011-32Y8L2H2FH router.

Partial breakout on the Cisco 8011-32Y8L2H2FH router:

- Enables flexible port combinations on platforms using H100 PHYs.
- Improves hardware utilization and bandwidth allocation.
- Allows to use both partial breakout and individual 100GE ports on the same PHY.

Partial breakout supported QSFP-DD optics

Lists the QSFP-DD optics that support partial breakout for enhanced connectivity options.

The following QSFP-DD optics support partial breakout:

- QDD-400G-DR4-S
- QDD-4X100G-FR-S
- QDD-4X100G-LR-S

[1] Cisco's high-speed physical layer (PHY) device used on platforms such as Cisco 8011-32Y8L2H2FH router to enable 200G and 400G Ethernet interfaces

Partial breakout examples for 400G optics

Provides examples of partial breakout configurationsfor 400 optics on Cisco 8010 Series routers, including how port and SerDes lane assignments are affected by different configurations.

With partial breakout enabled, if you configure 1x100G, 2x100G, or 3x100G on a port, say, Port 0 or Port 3, then the remaining SerDes lanes can be left unused and reassinged to other ports on the same Helium H100 PHY.

Without partial breakout, all four SerDes lanes are consumed by a single port, which blocks neighboring ports even if bandwidth is available.

This table provides some partial breakout examples.

The following table provide examples of partial breakout configurations.

Table 5: Partial breakout – Helium 1 PHY

Port 0	Port 1	Port 2
4x100G	-	-
3x100G	100	-
2x100G	100G	100G
2x100G	40G	40G
1x100G	100G	100G
1x100G	40G	40G

Table 6: Partial breakout – Helium 2 PHY

Port 3	Port 4	Port 5	Port 6	Port 7	Port 8	Port 9	Port 10	Port 11
4x100G	-	-	-	-	-	-	-	-
3x100G	50G	50G	-	-	-	-	-	-
2x100G	50G	50G	50G	50G	-	-	-	-
2x100G	10G/25G	10G/25G	10G/25G	10G/25G	-	-	-	-
1x100G	50G	50G	50G	50G	50G	50G	-	-
1x100G	10G/25G	10G/25G	10G/25G	10G/25G	50G	50G	-	-

Here, 100G supports 40G or 100G speed; 50G supports 10G, 25G, or 50G speed. Ports with a dash ('–') indicate disabled ports based on user configuration.

> **Note**
>
> Ports on the same quadrant share the same speed. For example, if Port 1 on one quadrant is configured with 100G speed, then Port 2 on the same quadrant should have 100G as the speed.

Partial breakout lane allocation for QSFP-DD modules

Provides details on how partial breakout allocates QSFP-DD lanes among multiple ports and example configuration.

In a typical deployment, partial breakout allows Port 0 to use only 2x100GE lanes from a 4x100GE QSFP-DD module, while remaining lanes are assigned to ports P1 and P2.

Example configuration for Port 0:

```
speed 200g
breakout 2x10
```

With this configuration, Port 0 operates using two 100GE lanes, freeing additional lanes for assignment to ports P1 and P2. This supports customized bandwidth allocation across ports in high-speed deployments.

5 Power management

Topics:

- NPU power optimization
- Dynamic power management
- Power redundancy protection
- On-demand transfer of redundant power modules to power reservation pool
- Ability to set maximum power limit for the router

Describes the router power management features, including NPU power optimization, dynamic power management, power redundancy protection, on-demand transfer of redundant power modules to the power reservation pool, and the configurable maximum power limit for the router.

This chapter describes the power management features on Cisco 8000 Series Routers and the procedures used to configure power optimization, redundancy, and power limits.

NPU power optimization

Describes the NPU power optimization feature, which lets an operator select a predefined power profile to reduce NPU power consumption based on network requirements.

NPU power optimization is a feature that lets you choose a predefined NPU power mode based on your network's individual requirements, and consequently reduces NPU power consumption.

Table 7: Feature history table

Feature Name	Release Information	Description
NPU Power Optimization	Release 25.4.1	Introduced in this release on: Fixed Systems (8010 [ASIC: A100])(select variants only*) *This feature is supported on: • 8011-32Y8L2H2FH • 8011-12G12X4Y-A/D
NPU Power Optimization	Release 25.1.1	Introduced in this release on: Fixed Systems (8700 [ASIC: K100], 8010 [ASIC: A100])(select variants only*) *This feature is supported on: • 8011-4G24Y4H-I • 8712-MOD-M
NPU Power Optimization	Release 24.4.1	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100])(select variants only*); Modular Systems (8800 [LC ASIC: P100])(select variants only*) *This feature is supported on: • 8212-48FH-M • 8711-32FH-M • 88-LC1-36EH • 88-LC1-12TH24FH-E • 88-LC1-52Y8H-EM
NPU Power Optimization	Release 7.3.15	This feature lets you choose a predefined NPU power mode based on your network's individual requirements, and consequently reducing NPU power consumption. The **hw-module npu-power-profile** command is introduced for this feature.

> **Note**
>
> The Cisco 8010 Series Routers do not support this feature. For a list of supported features on the Cisco 8010 Series Routers, see *Compatibility Matrix for Cisco 8010 Series Routers*.

Cisco 8000 series routers use Cisco Silicon One series processors. Cisco Silicon One processors offer high performance, flexible, and power-efficient routing silicon in the market.

NPU power optimization feature helps to reduce NPU power consumption by running a processor in a predefined mode. There are three NPU power modes–high, medium, and low.

Based on your network traffic and power consumption requirements, you can choose to run the processor in any one of the these NPU power modes:

- High: The router uses the maximum amount of power, resulting in the best possible performance.
- Medium: The router power consumption and performance levels are both average.
- Low: The router operates with optimal energy efficiency while providing a modest level of performance.

> **Note**
>
> We recommend that you work with your Cisco account representatives before implementing this feature in your network.

Configuration guidelines for NPU power optimization

Provides configuration guidelines for NPU power optimization.

These guidelines apply when you configure NPU power optimization feature:

NPU power mode configurations

- On a Q200-based Cisco 8200 series chassis, you can configure an NPU power mode on the entire router.
- On a Q200-based Cisco 8800 series chassis, you can configure an NPU power mode only on fabric cards and line cards.

Supported hardware and default modes

Supported Hardware	Default NPU Power Mode
Cisco 8200 32x400 GE 1RU fixed chassis (8201-32FH)	High
88-LC0-36FH without MACSec, based on Q200 Silicon Chip	Medium
88-LC0-36FH-M with MACSec, based on Q200 Silicon Chip	Medium
8808-FC0 Fabric Card, based on Q200 Silicon Chip	Low
8818-FC0 Fabric Card, based on Q200 Silicon Chip	Medium

> **Caution**
>
> We recommend that you use the default NPU power mode on your router.

Restrictions for NPU power mode

Lists the limitations of NPU power optimization, including its non-support on Q100-based systems and the specific Q200-based line cards that do not support the NPU Power Profile mode.

Support restrictions

- The NPU power optimization is not supported on the Q100-based systems.
- The NPU Power Profile mode is not supported on these Q200-based line cards:

Hardware and power profile modes restrictions

Hardware	Power Profile Mode
88-LC0-36FH-M	High
88-LC0-34H14FH	High

Configure NPU power mode

Describes how to configure the NPU power mode on the router so that the system applies the selected power profile and reduces NPU power consumption accordingly.

This task provides the procedures to configure and verify the NPU power mode on Cisco 8000 Series fixed and modular chassis.

Procedure

1. Configure NPU power mode on a fixed chassis.

   This example shows how to configure an NPU power mode on a fixed chassis:

   Example

```
Router(config)#hw-module npu-power-profile high
Router(config)#commit

Router(config)#reload
```

> **Note**
>
> Reload the chassis for the configurations changes to take effect.

2. Use the **show controllers npu driver** command to verify the NPU power mode configuration. The **NPU Power profile** field defines the NPU power mode.

   Example

```
Router#show controllers npu driver location 0/RP0/CPU0
Mon Aug 24 23:29:34.302 UTC
==========================================
NPU Driver Information
==========================================
Driver Version: 1
SDK Version: 1.32.0.1
Functional role: Active,     Rack: 8203, Type: lcc, Node: 0
Driver ready      : Yes
NPU first started : Mon Aug 24 23:07:41 2020
Fabric Mode:
NPU Power profile: High
Driver Scope: Node
Respawn count     : 1
Availablity masks :
        card: 0x1,     asic: 0x1,    exp asic: 0x1
...
```

3. Configure NPU power mode on a modular chassis.

   This example shows how to configure an NPU power mode on a fabric card and a line card:

   Example

```
Router(config)#hw-module npu-power-profile card-type FC high
Router(config)#hw-module npu-power-profile card-type LC low location 0/1/cpu0
Router(config)#commit
```

> **Note**
>
> For the configurations to take effect, you must:
>
> - Reload a line card if the configuration is applied on the line card.
> - Reload a router if the configuration is applied on a fabric card.

4. Verify the NPU power mode configuration on a modular chassis. Use the **show controllers npu driver location** command to verify the NPU power mode configuration. The **NPU Power profile** field defines the NPU power mode.

Example

```
Router#show controllers npu driver location 0/1/CPU0

Functional role: Active,     Rack: 8808, Type: lcc, Node: 0/RP0/CPU0
Driver ready      : Yes
NPU first started : Mon Apr 12 09:57:27 2021
Fabric Mode: FABRIC/8FC
NPU Power profile: High
Driver Scope: Rack
Respawn count     : 1
Availablity masks :
        card: 0xba,     asic: 0xcfcc,    exp asic: 0xcfcc
Weight distribution:
        Unicast: 80,      Multicast: 20
+-------------------------------------------------------------------+
| Process | Connection | Registration | Connection | DLL             |
| /Lib    | status     | status       | requests   | registration|
+-------------------------------------------------------------------+
| FSDB    | Active     | Active       |           1|  n/a            |
| FGID    | Active     | Active       |           1|  n/a            |
| AEL     | n/a        | n/a          |         n/a|  Yes             |
| SM      | n/a        | n/a          |         n/a|  Yes             |
+-------------------------------------------------------------------+

Asics :
HP - HotPlug event, PON - Power On reset
HR - Hard Reset,    WB  - Warm Boot
+-------------------------------------------------------------------------------+
| Asic inst. | fap|HP|Slice|Asic|Admin|Oper | Asic state | Last |PON|HR |
FW  |
|   (R/S/A)    | id |  |state|type|state|state|            | init |(#)|(#)|
Rev |
+-------------------------------------------------------------------------------+
| 0/FC1/2    | 202| 1| UP  |s123| UP  | UP  |NRML        |PON   |  1|
0|0x0000|
| 0/FC1/3    | 203| 1| UP  |s123| UP  | UP  |NRML        |PON   |  1|
0|0x0000|
| 0/FC3/6    | 206| 1| UP  |s123| UP  | UP  |NRML        |PON   |  1|
0|0x0000|
| 0/FC3/7    | 207| 1| UP  |s123| UP  | UP  |NRML        |PON   |  1|
0|0x0000|
| 0/FC4/8    | 208| 1| UP  |s123| UP  | UP  |NRML        |PON   |  1|
0|0x0000|
| 0/FC4/9    | 209| 1| UP  |s123| UP  | UP  |NRML        |PON   |  1|
0|0x0000|
| 0/FC5/10   | 210| 1| UP  |s123| UP  | UP  |NRML        |PON   |  1|
0|0x0000|
| 0/FC5/11   | 211| 1| UP  |s123| UP  | UP  |NRML        |PON   |  1|
0|0x0000|
| 0/FC7/14   | 214| 1| UP  |s123| UP  | UP  |NRML        |PON   |  1|
0|0x0000|
| 0/FC7/15   | 215| 1| UP  |s123| UP  | UP  |NRML        |PON   |  1|
0|0x0000|
+-------------------------------------------------------------------------------+

SI Info :
+-----------------------------------------------------------------------------------------+
|   Card  | Board      | SI Board | SI Param | Retimer SI    | Retimer SI
 | Front Panel   |
|         | HW Version | Version  | Version  | Board Version | Param Version
 | PHY           |
+-----------------------------------------------------------------------------------------+
```

```
|  FC1    |  0.22      |     1    |     6    |       NA       |       NA
 |       NA       |
|  FC3    |  0.21      |     1    |     6    |       NA       |       NA
 |       NA       |
|  FC4    |  0.21      |     1    |     6    |       NA       |       NA
 |       NA       |
|  FC5    |  0.21      |     1    |     6    |       NA       |       NA
 |       NA       |
|  FC7    |  0.21      |     1    |     6    |       NA       |       NA
 |       NA       |
+-------------------------------------------------------------------------------+
Functional role: Active,     Rack: 8808, Type: lcc, Node: 0/1/CPU0
Driver ready      : Yes
NPU first started : Mon Apr 12 09:58:10 2021
Fabric Mode: FABRIC/8FC
NPU Power profile: Low
Driver Scope: Node
Respawn count     : 1
Availablity masks :
        card: 0x1,     asic: 0x7,    exp asic: 0x7
Weight distribution:
        Unicast: 80,      Multicast: 20
```

Dynamic power management

Describes dynamic power management, which allocates router power based on the installed cards and operating modes, reduces the number of required power supply units, and improves overall PSU efficiency.

The Dynamic Power Management feature is a power allocation mechanism that

- considers dynamic factors, such as the type of fabric or line cards in the chassis, or the presence of a card in a slot before allocating power,
- optimizes total power distribution, and
- prevents overprovisioning of power to the router.

Table 8: Feature history table

Feature Name	Release Information	Description
Dynamic Power Management	Release 24.4.1	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100])(select variants only*); Modular Systems (8800 [LC ASIC: P100])(select variants only*) *This feature is supported on: • 8212-48FH-M • 8711-32FH-M • 88-LC1-36EH • 88-LC1-12TH24FH-E • 88-LC1-52Y8H-EM

Feature Name	Release Information	Description
Dynamic Power Management	Release 7.5.2	The Cisco 8202-32FH-M router will now consider dynamic factors, such as optical modules, NPU power profile, and MACsec mode to enable improved power allocation and use.
Dynamic Power Management	Release 7.3.15	The Dynamic Power Management feature considers certain dynamic factors before allocating power to the fabric and line cards. This feature has these benefits: • Reduces number of PSUs required by accurately representing the maximum power consumption • Improves PSU efficiency by providing more accurate power allocation This feature thus optimizes power allocation and avoids overprovisioning power to a router.
Dynamic Power Management	Release 7.3.3	The Dynamic Power Management feature is now supported on these Cisco 8100 and 8200 series routers: • Cisco 8201 • Cisco 8202 • Cisco 8201-32-FH • Cisco 8101-32-FH
Dynamic Power Management	Release 7.3.2	Previously available for fabric and line cards, this feature that helps avoid excess power allocation by considering dynamic factors before allocating power to them is now available for optical modules. To view the power allocation on a per port basis, a new command "**show environment power allocated [details]**" is introduced.

Benefits of dynamic power management

These are the benefits of using dynamic power management:

- Reduces number of PSUs required by accurately representing the maximum power consumption
- Improves PSU efficiency by providing more accurate power allocation
- Optimizes power allocation and avoids overprovisioning power to a router.

Configuration guidelines and restrictions for dynamic power management

Provides configuration guidelines and restrictions for the dynamic power management feature.

These guidelines apply to dynamic power management:

Supported platforms

- We recommend you work with your Cisco account representatives to calculate power requirements for the Cisco 8000 series router.
- The router enables this feature by default.
- The feature supports the following Cisco 8000 series routers and line cards:
  - Cisco 8804, Cisco 8808, Cisco 8812, and Cisco 8818 routers
  - Cisco 8201, Cisco 8202, Cisco 8201-32-FH, and Cisco 8202-32FH-M routers
  - Cisco 8101-32-FH
  - Cisco 8212-48FH-M
  - Cisco 8711-32FH-M
  - 88-LC1-36EH
  - 88-LC1-12TH24FH-E
  - 88-LC1-52Y8H-EM

Power allocation parameters

The dynamic power management feature allocates the total power to a router and its fabric card or line card based on these parameters:

- Number and type of fabric cards installed on the router
- Fabric cards operating modes (5FC or 8FC)
- Number and type of line cards installed on the router
- Combination of line card and fabric card types installed
- NPU power mode configured on a fabric card
- Number and type of optics installed (supported in IOS XR Release 7.3.2 and later)
- MACSec-enabled ports (supported from IOS XR 7.3.3 and later)

  For details, refer to *Dynamic Power Management for MACSec-Enabled Ports* section in the *Configuring MACSec* chapter in the *System Security Configuration Guide for Cisco 8000 Series Routers*.

On 8202-32FH-M router, the dynamic power management feature allocates the total power to a router based on these parameters:

- Optical modules installed.
- NPU power profile. To identify the mode on which the router is operating, use the `hw-module npu-power-profile` command.
- MACSec mode. By default, MACSec mode is disabled on 8202-32FH-M router.

> **Note**

Power allocation to empty card slot

Describes how the dynamic power management feature allocates a minimum required power to empty line card or fabric card slots so that the CPU and FPGAs can boot immediately when a card is inserted.

The power allocation for empty card slots is a power management mechanism that

- provides minimum power to empty line card or fabric card slots
- enables immediate boot-up of CPU and FPGAs upon card insertion, and
- facilitates card type detection before the system initiates data path power-up.

The feature allocates the minimum required power to all empty line card or fabric card slots. This power allows the CPU and FPGAs to boot immediately upon card insertion. The feature doesn't control booting up the CPU and FPGAs. Instead, the system uses this power to detect the card type before determining if sufficient power exists to activate the data path.

For example, the **show environment power** command output displays various LC or FC card statuses, and also shows allocated and used power.

> **Note**
>
> The allocated power capacity shown in this **show** command output isn't standard capacity. The allocated power capacity varies depending on various other factors.

```
Router# show environment power
Thu Apr 22 12:03:06.754 UTC
================================================================================
CHASSIS LEVEL POWER INFO: 0
================================================================================

   Total output power capacity (N + 1)             :    9600W +     6300W
   Total output power required                     :    9241W
   Total power input                               :    6146W
   Total power output                              :    5826W

================================================================================

   Power       Supply         -------Input--------   -----Output---     Status

   Module      Type             Volts A/B   Amps A/B   Volts     Amps

================================================================================

   0/PT0-PM0   PSU6.3KW-HV     245.5/245.7 5.1/5.0    54.7      43.1     OK
   0/PT0-PM1   PSU6.3KW-HV     0.0/245.2   0.0/7.4    54.3      31.7     OK
   0/PT0-PM2   PSU6.3KW-HV     0.0/246.9   0.0/7.5    54.1      32.3     OK

Total of Power Modules:       6146W/25.0A              5826W/107.1A

================================================================================

   Location     Card Type                Power       Power        Status
                                         Allocated   Used
                                         Watts       Watts

================================================================================

   0/RP0/CPU0   8800-RP                  95          69           ON
   0/RP1/CPU0   -                        95          -            RESERVED
   0/0/CPU0     88-LC0-36FH              796         430          ON
   0/1/CPU0     -                        102         -            RESERVED
   0/2/CPU0     88-LC0-36FH              796         430          ON
   0/3/CPU0     -                        102         -            RESERVED
```

```
0/4/CPU0      -                    102         -           RESERVED
0/5/CPU0      -                    102         -           RESERVED
0/6/CPU0      -                    102         -           RESERVED
0/7/CPU0      -                    102         -           RESERVED
0/8/CPU0      -                    102         -           RESERVED
0/9/CPU0      88-LC0-36FH          102         -           OFF
0/10/CPU0     -                    102         -           RESERVED
0/11/CPU0     -                    102         -           RESERVED
0/FC0         -                    26          -           RESERVED
0/FC1         -                    26          -           RESERVED
0/FC2         -                    26          -           RESERVED
0/FC3         8812-FC              784         509         ON
0/FC4         8812-FC              784         503         ON
0/FC5         8812-FC              26          -           OFF
0/FC6         8812-FC              26          -           OFF
0/FC7         8812-FC              26          -           OFF
0/FT0         8812-FAN             1072        1000        ON
0/FT1         8812-FAN             1072        1012        ON
0/FT2         8812-FAN             1072        861         ON
0/FT3         8812-FAN             1072        1033        ON
```

This table describes the card slot statuses:

Table 9: Router card slot status

Status	Description
RESERVED	When a slot is empty
OFF	When a card is inserted in a slot but power isn't allocated to the card
ON	When a card is allocated power and the card is in operational state

Low-power condition

Describes how the dynamic power management feature handles a low-power condition when the router lacks enough available power to provision a newly inserted line card or fabric card.

The low-power condition is a power management state that

- prevents power provisioning to new cards when resources are insufficient
- triggers the `ev_power_budget_not_ok` alarm, and
- initiates a graceful shutdown of the affected card.

When you insert an LC or FC in a card slot at the time when the router doesn't have enough power available to allocate to the new card, the dynamic power management feature doesn't provision power to the card. It raises the `ev_power_budget_not_ok` alarm, and gracefully shuts down the card.

This example shows the output of the **show shelfmgr history events location** command, which illustrates how the router gracefully shuts down an FC in the card slot *location 0/FC6* due to ack of power:

```
Router# show shelfmgr history events location 0/FC6
Thu Apr 22 12:03:11.763 UTC
```

```
NODE NAME     : 0/FC6
CURRENT STATE : CARD_SHUT_POWERED_OFF
TIME STAMP    : Apr 20 2021 16:49:52
------------------------------------------------------------------------------
DATE        TIME (UTC)  EVENT                    STATE
------------------------------------------------------------------------------
Apr 20 2021 16:49:52    ev_powered_off           CARD_SHUT_POWERED_OFF
Apr 20 2021 16:49:52    ev_device_offline        STATE_NOT_CHANGED
Apr 20 2021 16:49:52    ev_unmapped_event        STATE_NOT_CHANGED
Apr 20 2021 16:49:48    transient_condition      CARD_SHUTDOWN
Apr 20 2021 16:49:48    ev_check_card_down_reaso CHECKING_DOWN_REASON
Apr 20 2021 16:49:48    ev_timer_expiry          CARD_SHUTDOWN_IN_PROGRESS
Apr 20 2021 16:48:46    ev_power_budget_not_ok   CARD_SHUTDOWN_IN_PROGRESS
Apr 20 2021 16:48:45    transient_condition      POWER_BUDGET_CHECK
Apr 20 2021 16:48:45    ev_fpd_upgrade_not_reqd  CARD_STATUS_CHECK_COMPLETE
Apr 20 2021 16:47:45    ev_card_status_check     CARD_STATUS_CHECK
Apr 20 2021 16:47:45    ev_card_info_rcvd        CARD_INFO_RCVD
Apr 20 2021 16:47:44    ev_device_online         DEVICE_ONLINE
Apr 20 2021 16:47:43    ev_timer_expiry          CARD_POWERED_ON
Apr 20 2021 16:47:33    ev_powered_on            CARD_POWERED_ON
Apr 20 2021 16:47:33    init                     CARD_DISCOVERED
------------------------------------------------------------------------------
```

The router imposes the following limitations regarding power management and system reloads:

- The dynamic power management feature does not guarantee that previously operational LCs, FCs, optics, or interfaces will become active again following an LC, FC, or chassis reload.
- The router does not borrow power from a redundant power supply during a low-power condition.

Power allocation to optics

Describes how the dynamic power management feature reserves power for optical modules and shows how to identify the power allocated to a particular interface.

Power allocation for optics is a power management process that

- considers power requirements for optics during allocation
- automates power assignment upon the insertion of optical modules, and
- enables interface activation through the **no shut** command.

To identify the power allocated for a particular interface, use the **show environment power allocated [details] location** *location* command.

```
Router# show environment power allocated location 0/3/CPU0
Thu Oct  7 22:27:35.732 UTC
==============================================================================

   Location    Components              Power
                                       Allocated
                                       Watts
==============================================================================

  0/3/CPU0     Data-path               772
               OPTICS                  138
==============================================================================
```

```
               Total                     910
```

```
Router# show environment power allocated details location 0/3/CPU0
Thu Oct  7 22:27:42.221 UTC
================================================================================

   Location    Components                Power
                                         Allocated
                                         Watts
================================================================================

  0/3/CPU0     Data-path                 772
               0/3/0/0                   3
               0/3/0/1                   3
               0/3/0/2                   3
               0/3/0/3                   3
               0/3/0/4                   3
               0/3/0/5                   3
               0/3/0/6                   3
               0/3/0/7                   3
               0/3/0/8                   3
               0/3/0/9                   3
               0/3/0/10                  3
               0/3/0/11                  3
               0/3/0/12                  3
               0/3/0/13                  3
               0/3/0/14                  3
               0/3/0/15                  3
               0/3/0/16                  3
               0/3/0/17                  3
               0/3/0/18                  3
               0/3/0/19                  3
               0/3/0/20                  3
               0/3/0/21                  3
               0/3/0/22                  3
               0/3/0/23                  3
               0/3/0/24                  3
               0/3/0/25                  3
               0/3/0/26                  3
               0/3/0/27                  3
               0/3/0/28                  3
               0/3/0/29                  3
               0/3/0/30                  3
               0/3/0/31                  3
               0/3/0/32                  3
               0/3/0/33                  3
               0/3/0/34                  3
               0/3/0/35                  3
               0/3/0/36                  3
               0/3/0/37                  3
               0/3/0/38                  3
               0/3/0/39                  3
               0/3/0/40                  3
               0/3/0/41                  3
               0/3/0/42                  3
               0/3/0/43                  3
               0/3/0/44                  3
               0/3/0/46                  3
```

```
================================================================================

               Total                     910
```

The router provides specific feedback when power allocation fails:

- The system generates a `POWER ALLOCATION FAIL` syslog error and a major alarm when it lacks sufficient power to enable an optical module.

```
!<--Syslog Error-->!
#LC/0/3/CPU0:Oct  7 22:46:48.114 UTC: optics_driver[165]:
%PKT_INFRA-FM-3-FAULT_MAJOR : ALARM_MAJOR :POWER ALLOCATION FAIL :DECLARE
:0/3/CPU0:  Optics0/3/0/44
LC/0/3/CPU0:Oct  7 22:46:48.114 UTC: optics_driver[165]:
%L2-OPTICS-2-QSFP_POWER_ALLOCATION_FAILURE : Not enough power available to
enable Optics 0/3/0/44

!<--Alarm-->!
Router#show alarms brief system active
Thu Oct  7 22:47:19.569 UTC

------------------------------------------------------------------------------
Active Alarms
------------------------------------------------------------------------------
Location        Severity     Group            Set Time
Description
------------------------------------------------------------------------------
0/3/CPU0        Major        Software         10/07/2021 22:46:48 UTC
Optics0/3/0/44 - hw_optics:  Lack of available power to enable the optical
module
0/3/CPU0        Major        Software         10/07/2021 22:47:06 UTC
Optics0/3/0/46 - hw_optics:  Lack of available power to enable the optical
module
```

- The system displays a `PLATFORM-VEEA-1-PORT_NOT_ENABLED` syslog error if a user attempts to enable an interface using the `no shut` command without sufficient power allocation.

```
LC/0/2/CPU0:Aug 30 18:01:14.930 UTC: eth_intf_ea[262]:
%PLATFORM-VEEA-1-PORT_NOT_ENABLED : Power not allocated to enable the
interface HundredGigE0_2_0_6.
```

Power allocation to fixed-port routers

Describes how the dynamic power management feature allocates power on fixed-port Cisco 8000 series routers, with show environment power and show environment power allocated command examples.

The power allocation for fixed-port routers is a power management function that

- displays total power capacity and requirements
- identifies power allocated for specific interfaces, and
- provides granular power distribution data for router components.

This table describes the commands to monitor power metrics and their examples:This **show environment power** command output displays power information for fixed-port routers and components.

Command	Description	Example
`show environment power`	Use this command to view comprehensive power information for the chassis and its components.	

Command	Description	Example

```
Router# show environment power
Wed Feb 16 21:05:10.001 UTC
=============================================================

CHASSIS LEVEL POWER INFO: 0
=============================================================

   Total output power capacity (Group 0 + Grou
 +     1400W
   Total output power required

   Total power input

   Total power output

Power Group 0:
=============================================================

   Power       Supply         ------Input----
     Status
   Module      Type             Volts     Amps
Amps
=============================================================

   0/PM0       PSU1.4KW-ACPE    244.5     0.8
11.1     OK

Total of Group 0:               195W/0.8A

Power Group 1:
=============================================================

   Power       Supply         ------Input----
     Status
   Module      Type             Volts     Amps
Amps
=============================================================

   0/PM1       PSU1.4KW-ACPE    244.2     0.8
10.2     OK

Total of Group 1:               195W/0.8A

=============================================================

   Location     Card Type                Power
    Status
                                         Alloca
                                         Watts
=============================================================

   0/RP0/CPU0   8201                     893
    ON
   0/FT0        FAN-1RU-PE               28
    ON
   0/FT1        FAN-1RU-PE               28
    ON
   0/FT2        FAN-1RU-PE               28
    ON
   0/FT3        FAN-1RU-PE               28
    ON
```

Command	Description	Example
		0/FT4 FAN-1RU-PE 28 ON
show environment power allocated details location*location*	Use this command command to identify the power allocated for a particular interface.	Router# **show environment power allocated locat** Wed Feb 16 21:05:21.360 UTC Location Components Power Alloca Watts 0/RP0/CPU0 Data-path 858 **OPTICS** **35** Total 893
		Router# **show environment power allocated detai** **0/RP0/CPU0** Wed Feb 16 21:05:36.142 UTC Location Components Power Alloca Watts 0/RP0/CPU0 Data-path 858 **0/0/0/19** **21** **0/0/0/18** **14** Total 893

Disable dynamic power management

Describes how to disable dynamic power management on the router, which is enabled by default.

By default, the dynamic power management is enabled on a router. This example shows how to disable dynamic power management:

Procedure

1. Enter the global configuration mode.

   Example

   ```
   Router# configure
   ```

2. Use the **power-mgmt action disable** command to disable dynamic power management.

   Example

   ```
   Router(config)#power-mgmt action disable
   ```

3. Save the changes.

   Example

   ```
   Router(config)#commit
   ```

   > **Caution**
   >
   > After disabling the dynamic power management feature, you must manage the router power on your own. So, use this command with caution.

4. To enable dynamic power management again, use the **no power-mgmt action disable** command.

Power redundancy protection

Describes the power redundancy protection feature, which raises an alarm when the required output power exceeds the total feed redundancy capacity, and explains the single-fault and dual-fault protection modes.

The power redundancy protection is a power management mechanism that

- ensures continuous router operation during power supply failures
- provides power feed redundancy through A and B feeds, and
- triggers alarms when power requirements exceed capacity.

The Cisco 8000 Series Modular Routers utilize two primary redundancy mechanisms to maintain functionality during power supply failures:

- PSU redundancy incorporates extra power supply units that takes over the load if a failure occurs.
- Power feed redundancy divides input power into A and B feeds. When both feeds function normally, they share the power load equally. If one feed fails, the remaining feed scales up to its maximum capacity or the power supply unit operates with reduced input to maintain an uninterrupted power supply.

Table 10: Feature history table

Feature Name	Release Information	Feature Description
Power Redundancy Protection	Release 25.4.1	Introduced in this release on: Fixed Systems (8010 [ASIC: A100])(select variants only*) *This feature is supported on: • 8011-32Y8L2H2FH • 8011-12G12X4Y-A/D
Power Redundancy Protection	Release 25.1.1	Introduced in this release on: Fixed Systems (8700 [ASIC: K100], 8010 [ASIC: A100])(select variants only*) *This feature is supported on: • 8011-4G24Y4H-I • 8712-MOD-M
Power Redundancy Protection	Release 24.4.1	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100])(select variants only*); Modular Systems (8800 [LC ASIC: P100])(select variants only*) *This feature is supported on: • 8212-48FH-M • 8711-32FH-M • 88-LC1-36EH • 88-LC1-12TH24FH-E • 88-LC1-52Y8H-EM

Feature Name	Release Information	Feature Description
Power Redundancy Protection	Release 24.1.1	You can now prevent power module exhaustion or failure due to power redundancy issues in the power feeds with the help of alarms that warn that the total output power required by the router exceeds the total feed redundancy capacity. You can configure either single-fault protection or dual fault protection, depending on whether you want to trigger alarms during redundancy failures in the power supply feed, PSU redundancy, or both. The feature introduces these changes: CLI: • **power-mgmt feed-redundancy** • The `Total feed redundancy capacity` field is added to the **show environment** command.

These options provide high reliability and minimize the risk of network downtime. The routers incorporate protection that triggers alarms for PSU and feed redundancy failures when the total output power required exceeds the total feed redundancy capacity.

The router supports two redundancy configuration modes:

- Single fault protection - this mode monitors the router against a single power supply feed or PSU redundancy failure.
- Dual fault protection - this mode monitors the router against a power supply feed and PSU redundancy failure simultaneously.

You can customize the PSU single feed capacity within a default power range to meet specific infrastructure requirements. The router determines the total feed capacity by selecting the lesser value between the feed redundancy capacity and the PSU redundancy capacity. The PSU redundancy capacity is the number of power supply units minus the redundant ones (N) multiplied by a dual feed capacity. On the other hand, the feed redundancy capacity is the total number of PSUs multiplied by a single feed capacity. In single-fault protection, the PSU refers to the total number of power supply units in the router units (N+1). In dual-fault protection, the PSU refers to the number of power supply units minus the redundant ones (N).

For example, consider a router that has a total of 9 PSUs with a default N + 1 power redundancy configuration. The PSU feed capacity with dual feed is 4800 W and the single feed capacity value is set 3200 W, then the total feed redundancy capacity would be:

Table 11: Total feed redundancy capacity example

Power Redundancy Protection	Total Number of PSUs	PSU redundancy	Number of PSUs minus the redundant ones (N)	Dual Feed Capacity	Single Feed Capacity	Feed Redundancy Capacity	PSU Redundancy Capacity	Total Feed Redundancy Capacity
Single fault protection	9	N+1	8	4800 W	3200 W	28800 W	38400 W	28800 W
Dual fault protection	9	N+1	8	4800 W	3200 W	25600 W	38400 W	25600 W

Guidelines and restrictions for power redundancy protection

Lists the guidelines and restrictions that apply to the power redundancy protection feature on the router.

- By default, the router doesn't enable Power Redundancy Protection.
- The Power Redundancy Protection feature doesn't impact the power budgeting in the routers.
- For maximum power redundancy protection, use the dual fault protection.
- For total feed redundancy capacity calculations, the router considers only the PSUs with A and B inputs. Both A and B inputs must be within the operating range in healthy conditions. If either feed is unavailable, the router excludes such PSUs from the calculations.
- The router considers all PSUs, including redundant PSUs with two feeds (within the operating range in healthy condition) for feed redundancy capacity in single fault protection. However, the router excludes the redundant PSUs for feed redundancy capacity in dual fault protection. If the router has 8 PSUs and N+3 redundancy, single fault protection calculation considers all eight PSUs, whereas dual fault protection considers just 5 PSUs.

Configure single fault protection

Describes how to configure single-fault power redundancy protection on the router by setting the PSU single feed capacity, so that the system raises an alarm when the required output power exceeds the redundancy capacity.

Use the **power-mgmt feed-redundancy** command to configure the power redundancy protection mode and PSU single feed capacity.

Procedure

1. Enter the global configuration mode.

   Example

   ```
   Router# configure
   ```

2. Configure single fault protection with PSU single feed capacity set to 2400 Watts.

Example

```
Router(config)# power-mgmt feed-redundancy single-fault-protection capacity
2400
```

3. Save the changes.

Example

```
Router(config)# commit
```

4. Use the **show run power** command to check the running configuration.

Example

```
Router# show run power
…
power-mgmt feed-redundancy single-fault-protection capacity 2400
…
```

5. Use the **show environment power** command to verify the total power required and the total feed capacity for single fault protection.

Example

```
Router# show env power
=============================================================================
CHASSIS LEVEL POWER INFO: 0
=============================================================================

   Total output power capacity (N + 1)             :   28800W +     4800W
   Total output power required                     :    6679W >>>>> 1
   Total power input                               :    2394W
   Total power output                              :    2066W
   Total feed redundancy capacity (Single Fault)   :   16800W >>>>> 2
   //*The router triggers feed redundancy loss alarm when 1 > 2.**//
=============================================================================

   Power       Supply        -------Input--------   -----Output---     Status

   Module       Type             Volts A/B   Amps A/B   Volts     Amps
=============================================================================

   0/PT0-PM0   PSU4.8KW-DC100  62.8/62.7   2.6/2.5    55.2      5.3      OK
   0/PT0-PM1   PSU4.8KW-DC100  62.7/62.7   2.7/2.6    55.3      5.3      OK
   0/PT0-PM3   PSU4.8KW-DC100  61.0/62.7   2.6/2.5    55.2      4.8      OK
   0/PT1-PM0   PSU4.8KW-DC100  67.3/67.3   2.7/2.5    55.3      5.2      OK
   0/PT1-PM1   PSU4.8KW-DC100  67.3/67.2   2.8/2.7    55.3      5.7      OK
   0/PT1-PM2   PSU4.8KW-DC100  67.3/67.4   2.7/2.7    55.2      5.6      OK
   0/PT1-PM3   PSU4.8KW-DC100  67.3/67.3   2.6/2.5    55.3      5.5      OK

Total of Power Modules:       2394W/36.7A              2066W/37.4A
```

Configure dual fault protection

Describes how to configure dual-fault power redundancy protection on the router by setting the PSU single feed capacity, and how to view alarms and syslog messages raised when the required output power exceeds the redundancy capacity.

Use the **power-mgmt feed-redundancy** command to configure the power redundancy protection mode and PSU single feed capacity.

Procedure

1. Enter the global configuration mode.

   Example

   ```
   Router# configure
   ```

2. Configure dual fault protection with PSU single feed capacity set to 2400 Watts.

   Example

   ```
   Router(config)# power-mgmt feed-redundancy dual-fault-protection capacity
   2400
   ```

3. Save the changes.

   Example

   ```
   Router(config)# commit
   ```

4. Use the **show run power** command to check the running configuration.

   Example

   ```
   Router# show run power
   …
   power-mgmt feed-redundancy dual-fault-protection capacity 2400
   …
   ```

5. Use the **show environment power** command to verify the total power required and the total feed capacity for dual fault protection.

   Example

   ```
   Router# show env power
   ================================================================================
   CHASSIS LEVEL POWER INFO: 0
   ================================================================================

      Total output power capacity (N + 1)             :   28800W +     4800W
      Total output power required                     :    6679W >>>>> 1
      Total power input                               :    2394W
      Total power output                              :    2066W
      Total feed redundancy capacity (Dual Fault)     :   14400W >>>>> 2
    //*The router triggers feed redundancy loss alarm when 1 > 2.**//
   ```

```
==============================================================================

   Power       Supply         -------Input--------   -----Output---     Status

   Module      Type             Volts A/B   Amps A/B   Volts     Amps

==============================================================================

   0/PT0-PM0   PSU4.8KW-DC100   62.8/62.7   2.6/2.5    55.2      5.3       OK
   0/PT0-PM1   PSU4.8KW-DC100   62.7/62.7   2.7/2.6    55.3      5.3       OK
   0/PT0-PM3   PSU4.8KW-DC100   61.0/62.7   2.6/2.5    55.2      4.8       OK
   0/PT1-PM0   PSU4.8KW-DC100   67.3/67.3   2.7/2.5    55.3      5.2       OK
   0/PT1-PM1   PSU4.8KW-DC100   67.3/67.2   2.8/2.7    55.3      5.7       OK
   0/PT1-PM2   PSU4.8KW-DC100   67.3/67.4   2.7/2.7    55.2      5.6       OK
   0/PT1-PM3   PSU4.8KW-DC100   67.3/67.3   2.6/2.5    55.3      5.5       OK

Total of Power Modules:       2394W/36.7A              2066W/37.4A
```

6. You can use the **show alarms brief** command to view the power redundancy alarm.

Example

```
Router# show alarms brief system active
------------------------------------------------------------------------------
Active Alarms
------------------------------------------------------------------------------
Location        Severity     Group           Set Time
Description



------------------------------------------------------------------------------



0               Major        Environ         11/27/2023 12:55:08 UTC    Power
 Module redundancy feed mode lost
```

Note

The router triggers the `Power Module redundancy feed mode lost` alarm only when Total output power required exceeds Total feed redundancy capacity.

7. View system log messages for power redundancy loss.

Example

Syslog message created while power redundancy loss (total output power exceeds total feed redundancy capacity):

```
RP/0/RP0/CPU0:Dec 15 10:24:29.489 UTC: envmon [123]:
%PKT_INFRA-FM-3-FAULT_MAJOR : ALARM_MAJOR :Power Feed redundancy lost :DECLARE
 :0
```

On-demand transfer of redundant power modules to power reservation pool

Describes how Cisco 8800 Modular Routers transfer redundant power supply units to the power reservation pool on demand to meet component requirements.

The on-demand transfer of redundant power modules to power reservation pool is a power management process that

- prioritizes component power requirements over redundancy preservation
- transfers redundant power modules to the power reservation pool on demand, and
- restores redundancy automatically when power consumption decreases.

Table 12: Feature history table

Feature Name	Release Information	Feature Description
On-demand transfer of Redundant Power Modules to Power Reservation Pool	Release 25.4.1	Introduced in this release on: Fixed Systems (8010 [ASIC: A100])(select variants only*) *This feature is supported on: • 8011-32Y8L2H2FH • 8011-12G12X4Y-A/D
On-demand transfer of Redundant Power Modules to Power Reservation Pool	Release 25.1.1	Introduced in this release on: Fixed Systems (8700 [ASIC: K100], 8010 [ASIC: A100])(select variants only*) *This feature is supported on: • 8712-MOD-M • 8011-4G24Y4H-I
On-demand transfer of Redundant Power Modules to Power Reservation Pool	Release 24.4.1	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100])(select variants only*); Modular Systems (8800 [LC ASIC: P100])(select variants only*) *This feature is now supported on: • 8212-48FH-M • 8711-32FH-M • 88-LC1-12TH24FH-E • 88-LC1-36EH • 88-LC1-52Y8H-EM

Feature Name	Release Information	Feature Description
On-demand transfer of Redundant Power Modules to Power Reservation Pool	Release 7.11.1	The Cisco 8800 Series Modular Routers now have a functionality that allows them to transfer their redundant Power Supply Units (PSUs) to the power reservation pool when there is inadequate power supply. This capability helps prevent the router from shutting down hardware components due to a lack of power in the reservation pool, which used to occur due to the router prioritizing redundancy over power availability in the power reservation pool. Consequently, the router now raises an alarm indicating redundancy loss when it transfers PSUs to the power reservation pool. This feature ensures that the router components reserve the necessary power, even when redundancy is enabled.

Cisco 8000 Series Modular Routers provide redundancy while managing Power Supply Units (PSUs) to ensure continuous operation. By default, the router operates in N+1 redundancy, where N represents the number of PSUs allotted to the power reservation pool and 1 indicates the backup PSU. Administrators configure the PSU redundancy from N+1 to N+x using the `power-mgmt redundancy-num-pms` command, where x represents the number of redundant PSUs. The system requires that the total number of functioning PSUs remains at least x more than the number of PSUs required to support the power demanded by all system components.

The Cisco 8000 Series Modular Routers offer redundancy while managing Power Supply Units (PSUs), providing continuous operation if there is PSU failure. By default, the router operates in N+1 redundancy, where N represents the number of PSUs allotted to the power reservation pool for powering the router components, and 1 indicates the backup PSU. You can use the **power-mgmt redundancy-num-pms** *number* command in the XR config mode to configure the PSU redundancy from N+1 to N+x, where x is the number of redundant PSUs required. The total number of functioning PSUs must be at least x more than the number of PSUs required to support the power demanded by all the components in the system for optimal router functionality. The range of values assigned to x is 0–11, where 0 implies no power redundancy. The router uses the redundant PSUs only when there is a PSU failure. But, if the power requirement of the router increases than the available power offered by PSUs, the router prioritizes maintaining PSU redundancy overpowering the components.

Cisco 8800 Modular Routers prioritize powering router components over maintaining redundancy. When the power requirement exceeds the available power in the reservation pool, the router transfers redundant PSUs to the power reservation pool to meet demand. The system automatically restores redundancy and clears the associated alarm if subsequent actions reduce power consumption.

For example, consider a scenario with 18900W (3 6300W PSUs) available power. Initially, the router reserves 12600W (using 2 PSUs) in the power reservation pool and retains 6300W (one PSU) as a backup to maintain N+1 redundancy. Suppose the router needs to reserve power for any components to power up and needs more power than is available in the reservation pool. In that case, the router uses the entire 18900W with all three PSUs to power the components by transferring the redundant PSU to the power reservation pool. The router then triggers a redundancy loss alarm with such an assignment. However, if any further actions result in reduced power consumption in the router, the system automatically restores redundancy and clears the redundancy lost alarm.

The router provides the following monitoring and verification capabilities:

- On redundancy loss, the router raises a **Critical** severity **Power Module redundancy lost** alarm. You can use the **show alarms brief** command to view the redundancy lost alarm.

- Syslog message created while redundancy loss (transforming redundant PSU to functional PSU):

```
RP/0/RP0/CPU0:Jul 24 11:49:01.316 UTC: envmon[214]:
%PKT_INFRA-FM-3-FAULT_MAJOR : ALARM_MAJOR :Power Module redundancy lost
:DECLARE :0:
```

- Syslog message created while restoring redundancy:

```
RP/0/RP0/CPU0:Jul 24 11:49:11.375 UTC: envmon[214]:
%PKT_INFRA-FM-3-FAULT_MAJOR : ALARM_MAJOR :Power Module redundancy lost :CLEAR
 :0:
```

- Use the **show environment** view the redundancy status of the PSUs in the router.

Verify the redundancy status in the router

This section details the commands to verify the redundancy status in the router:

Router with N+1 redundancy:

```
Router:ios# show environment power

================================================================================

            CHASSIS LEVEL POWER INFO: 0

================================================================================

            Total output power capacity (N + 1)             :   12600W +
6300W
            Total output power required                     :   11545W
            Total power input                               :    3302W
            Total power output                              :    3004W


================================================================================

            Power       Supply         -------Input--------   -----Output---
    Status
            Module      Type            Volts A/B   Amps A/B   Volts     Amps


================================================================================

            0/PT5-PM0   PSU6.3KW-HV     240.5/241.3 2.2/2.4    55.1      18.3
     OK
            0/PT5-PM1   PSU6.3KW-HV     240.5/240.8 2.1/2.3    54.8      17.3
     OK
            0/PT5-PM2   PSU6.3KW-HV     242.2/241.1 2.3/2.4    54.9      19.1
     OK

           Total of Power Modules:       3302W/13.7A              3004W/54.7A


================================================================================

            Location     Card Type               Power       Power
Status
            Allocated   Used
            Watts       Watts
```

```
==============================================================================

            0/RP0/CPU0   8800-RP                 105         78           ON
            0/RP1/CPU0   -                       105         -
RESERVED
            0/0/CPU0     8800-LC-36FH            1097        513          ON
            0/1/CPU0     -                       102         -
RESERVED
            0/2/CPU0     88-LC0-36FH             102         0            OFF

            0/3/CPU0     -                       102         -
RESERVED
            0/4/CPU0     -                       102         -
RESERVED
            0/5/CPU0     -                       102         -
RESERVED
            0/6/CPU0     -                       102         -
RESERVED
            0/7/CPU0     -                       102         -
RESERVED
            0/8/CPU0     -                       102         -
RESERVED
            0/9/CPU0     -                       102         -
RESERVED
            0/10/CPU0    -                       102         -
RESERVED
            0/11/CPU0    -                       102         -
RESERVED
            0/12/CPU0    -                       102         -
RESERVED
            0/13/CPU0    -                       102         -
RESERVED
            0/14/CPU0    -                       102         -
RESERVED
            0/15/CPU0    -                       102         -
RESERVED
            0/16/CPU0    -                       102         -
RESERVED
            0/17/CPU0    -                       102         -
RESERVED
            0/FC0        -                       32          -
RESERVED
            0/FC1        -                       32          -
RESERVED
            0/FC2        8818-FC0                584         475          ON
            0/FC3        -                       32          -
RESERVED
            0/FC4        8818-FC0                584         472          ON
            0/FC5        -                       32          -
RESERVED
            0/FC6        -                       32          -
RESERVED
            0/FC7        -                       32          -
RESERVED
            0/FT0        8818-FAN                1786        237          ON
            0/FT1        8818-FAN                1786        228          ON
            0/FT2        8818-FAN                1786        234          ON
            0/FT3        8818-FAN                1786        228          ON
```

Router with redundancy loss:

```
Router:ios# sh env power

==============================================================================

            CHASSIS LEVEL POWER INFO: 0

==============================================================================

            Total output power capacity (N + 1)             :   18900W +
   0W
            Total output power required                     :   12689W
            Total power input                               :    3302W
            Total power output                              :    3004W


==============================================================================

            Power       Supply         -------Input--------   -----Output---
    Status
            Module      Type            Volts A/B   Amps A/B   Volts     Amps


==============================================================================

            0/PT5-PM0   PSU6.3KW-HV     240.5/241.3 2.2/2.4    55.1      18.3
     OK
            0/PT5-PM1   PSU6.3KW-HV     240.5/240.8 2.1/2.3    54.8      17.3
     OK
            0/PT5-PM2   PSU6.3KW-HV     242.2/241.1 2.3/2.4    54.9      19.1
     OK

           Total of Power Modules:       3302W/13.7A              3004W/54.7A


==============================================================================

            Location     Card Type               Power       Power
Status
            Allocated   Used
            Watts       Watts

==============================================================================

            0/RP0/CPU0   8800-RP                 105         78           ON
            0/RP1/CPU0   -                       105         -
RESERVED
            0/0/CPU0     8800-LC-36FH            1097        513          ON
            0/1/CPU0     -                       102         -
RESERVED
            0/2/CPU0     88-LC0-36FH             916         510          ON
            0/3/CPU0     -                       102         -
RESERVED
            0/4/CPU0     -                       102         -
RESERVED
            0/5/CPU0     -                       102         -
RESERVED
            0/6/CPU0     -                       102         -
RESERVED
            0/7/CPU0     -                       102         -
RESERVED
```

```
            0/8/CPU0     -                          102          -
RESERVED
            0/9/CPU0     -                          102          -
RESERVED
            0/10/CPU0    -                          102          -
RESERVED
            0/11/CPU0    -                          102          -
RESERVED
            0/12/CPU0    -                          102          -
RESERVED
            0/13/CPU0    -                          102          -
RESERVED
            0/14/CPU0    -                          102          -
RESERVED
            0/15/CPU0    -                          102          -
RESERVED
            0/16/CPU0    -                          102          -
RESERVED
            0/17/CPU0    -                          102          -
RESERVED
            0/FC0        -                          32           -
RESERVED
            0/FC1        -                          32           -
RESERVED
            0/FC2        8818-FC0                   749          475          ON
            0/FC3        -                          32           -
RESERVED
            0/FC4        8818-FC0                   749          472          ON
            0/FC5        -                          32           -
RESERVED
            0/FC6        -                          32           -
RESERVED
            0/FC7        -                          32           -
RESERVED
            0/FT0        8818-FAN                   1786         237          ON
            0/FT1        8818-FAN                   1786         225          ON
            0/FT2        8818-FAN                   1786         234          ON
            0/FT3        8818-FAN                   1786         228          ON
```

```
Router:ios# sh alarms brief system active

------------------------------------------------------------------------------

            Active Alarms

------------------------------------------------------------------------------

            Location        Severity     Group            Set Time
        Description

------------------------------------------------------------------------------

            0/RP0/CPU0      Critical     Software         10/27/2023 00:22:08
 UTC    Redundancy Partner Not Present
            0               Major        Environ          10/27/2023 00:23:48
 UTC    Power Module redundancy lost
            0/RP0/CPU0      Minor        Fabric           10/27/2023 00:22:39
 UTC    Fabric Plane-0 status
            0/RP0/CPU0      Minor        Fabric           10/27/2023 00:22:39
 UTC    Fabric Plane-1 status
            0/RP0/CPU0      Minor        Fabric           10/27/2023 00:22:39
 UTC    Fabric Plane-3 status
```

```
          0/RP0/CPU0      Minor        Fabric           10/27/2023 00:22:39
UTC    Fabric Plane-5 status
          0/RP0/CPU0      Minor        Fabric           10/27/2023 00:22:39
UTC    Fabric Plane-6 status
          0/RP0/CPU0      Minor        Fabric           10/27/2023 00:22:39
UTC    Fabric Plane-7 status
          0/RP0/CPU0      Major        Software         10/27/2023 00:22:59
UTC    Communications Failure With Cisco Licensing Cloud
          0               Major        Environ          10/27/2023 00:23:48
UTC    Power Module redundancy lost
```

Ability to set maximum power limit for the router

Describes the **power-mgmt configured-power-capacity** command.

The ability to set maxinum power limit for the router is a power management feature that

- prevents power consumption from exceeding infrastructure capacity
- mitigates the risk of system brownouts, and
- enables administrators to restrict router power usage based on specific infrastructure requirements.

Table 13: Feature history table

Feature Name	Release Information	Feature Description
Ability to Set Maximum Power Limit for the Router	Release 25.4.1	Introduced in this release on: Fixed Systems (8010 [ASIC: A100])(select variants only*) *This feature is supported on: • 8011-32Y8L2H2FH • 8011-12G12X4Y-A/D
Ability to Set Maximum Power Limit for the Router	Release 25.1.1	Introduced in this release on: Fixed Systems (8700 [ASIC: K100], 8010 [ASIC: A100])(select variants only*) *This feature is supported on: • 8011-4G24Y4H-I • 8712-MOD-M
Ability to Set Maximum Power Limit for the Router	Release 24.4.1	Introduced in this release on: Fixed Systems(8200, 8700); Modular Systems (8800 [LC ASIC: P100]) (select variants only*). *This feature is now supported on: • 8212-32FH-M • 8711-32FH-M • 88-LC1-12TH24FH-E

Feature Name	Release Information	Feature Description
Ability to Set Maximum Power Limit for the Router	Release 7.11.1	We are introducing functionality to set the maximum power limit for a router to improve power management and distribution in the PSUs. It prevents a router from using more than the configured power and also gives the ability to limit the reservation pool regardless of how many power supplies are present. In the previous releases, the ability to prevent a router from using more than a configured amount of power was unavailable. This feature introduces this change: CLI • **power-mgmt configured-power-capacity**

Guidelines and restrictions for setting maximum power limit for the router

These guidelines and restrictions apply when you set maximum power limit for the router:

- The ability to set maxinum power limit feature is not applicable to fixed-port routers.
- With this feature, you can manage system power based on a configured maximum power capacity. This ensures that the router does not allocate more power than the infrastructure supports.
- It also gives you the ability to limit power to a router according to your infrastructure requirements. The max power capacity parameter doesn't allow power consumed by the hardware to cross the configured amount.
- The criteria to set maximum power limit is that the value must be set between the current allocated power and the available maximum power at time of configuration.
- You must set the maximum power limit value between the current allocated power and the maximum power available at the time of configuration.
- The `power-mgmt configured-power-capacity` command allows the configuration of the maximum power limit.
- The **PKT_INFRA-FM-3-FAULT_MAJOR : ALARM_MAJOR :Power reservation exceeds configured power** alarm alerts administrators when the power reservation exceeds the configured maximum power capacity.

> **Note**
>
> This alarm is extremely rare and triggers only when hardware, such as a fan tray, is inserted and granted power without a specific request.

6 Fault detection, recovery, and diagnostics

Topics:

- Fabric link management for uncorrectable errors
- Fault recovery handling
- Periodic syslog messages for shutdowns due to fault-recovery failures
- Machine check error notifications

Describes the fault detection, recovery, and diagnostic features of Cisco 8000 Series Routers, including fabric link management for uncorrectable errors, configurable fault recovery attempts, periodic shutdown syslog messages, and procedures for viewing machine check error details.

This chapter describes the fault detection, recovery, and diagnostic features on Cisco 8000 Series Routers, and the procedures used to monitor fabric links, control fault recovery attempts, and view machine check error details.

Fabric link management for uncorrectable errors

Describes how the router uses Forward Error Correction (FEC) to detect uncorrectable errors on fabric links, retune noisy links, and permanently shuts down a link after repeated failures.

Forward Error Correction (FEC) is a error control method in data transmission that

- allows the transmitter to send redundant data so the receiver can recognize only the portion of the data that contains no apparent errors, and
- enables the receiver to detect and correct a limited number of errors.

The Cisco IOS XR router will not bring the link to the data plane if the link is noisy at inception or during bring up. If the link becomes noisy after it is brought up, the fabric link will be reset and re-tuned. If this event occurs five times within an hour, the fabric link shuts down permanently. After the link is up, the polling interval for link error is 10 minutes.

Fabric link management feature uses FEC as the criteria to determine if a link is good. The router receives a notification for every bad FEC on each fabric port. FEC can correct up to 15 bit errors; beyond this threshold, the error is considered uncorrectable. This feature allows fabric links to operate without errors.

In Cisco IOS XR Release 24.2.11, the FEC feature is enabled only on Q200-based line cards and fabric cards.

Table 14: Feature history table

Feature Name	Release Information	Feature Description
Fabric Link Management for Uncorrectable Errors	Release 25.4.1	Introduced in this release on: Fixed Systems (8010 [ASIC: A100])(select variants only*) *This feature is supported on: • 8011-32Y8L2H2FH • 8011-12G12X4Y-A/D
Fabric Link Management for Uncorrectable Errors	Release 25.1.1	Introduced in this release on: Fixed Systems (8700 [ASIC: K100], 8010 [ASIC: A100])(select variants only*) *This feature is supported on: • 8011-4G24Y4H-I • 8712-MOD-M

Feature Name	Release Information	Feature Description
Fabric Link Management for Uncorrectable Errors	Release 24.4.1	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100])(select variants only*); Modular Systems (8800 [LC ASIC: P100])(select variants only*) *This feature is supported on: • 8212-48FH-M • 8711-32FH-M • 88-LC1-36EH • 88-LC1-12TH24FH-E • 88-LC1-52Y8H-EM
Fabric Link Management for Uncorrectable Errors	Release 24.2.11	You can now run your fabric links error-free using the forward error correction (FEC) technique. The feature allows you to determine the link quality by monitoring the noisy fabric links during and post bring-up. This feature introduces the **hw-module fabric-fec-monitor disable** command.

FEC bin index

The FEC bin index indicates the number of bit errors.

For example, FEC bin index of a good link is {12642341946,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,} and for a bad link it is {221568554,532162,414888,101277,144171,3317,61681,4065,741,1977586,138,62,17,6,1,}.

If the FEC bin index is equal to or greater than ten non-zero bits (bin ≥ 10 non-zero) before the link is up, the FEC will indicate that the link is bad. When the link is up and the FEC bin index is equal to or greater than 13 non-zero bits (bin ≥ 13 non-zero), the FEC will indicate that the link is bad.

Link states for a noisy fabric link

When a fabric link is noisy, any of these link states is possible:

- Link does not come up at all.
- Link comes up, but fluctuates.
- Link comes up, but generates uncorrectable errors.

The network traffic flow is not affected if the link never comes up; however, packet drops may occur in the other two link states.

How the router monitors FEC fabric links

Describes the sequence the router follows for each FEC report to monitor fabric links, including link retuning, MAC port re-activation after repeated failures, and permanent shutdown after the sixth failure within an hour.

Summary

The key components involved in the fabric link monitoring process are:

- Router: A network device that monitors fabric links by processing FEC reports, performing retuning, logging system messages, and managing link states based on failure frequency.
- Fabric link: A physical connection that undergoes quality monitoring, retuning, and snapshot collection to ensure stable data plane operation, with a permanent shutdown occurring after the sixth failure within one hour.
- MAC port: A network interface that stops and reactivates between the second and fifth link failure to facilitate recovery.

Workflow

For every FEC report, the router performs this process to monitor the fabric links:

1. If the fabric link is faulty before the link is up, the router retunes and checks again for the FEC improvement.
2. If the link quality does not improve after retuning, the router displays the syslog message after tuning for 100 times and does not bring the link to the data plane.
3. Post link up, when the fabric link becomes noisy, the router collects a snapshot and retunes after the first failure.
4. From second failure to fifth failure, the MAC port stops and re-activates. Retune is done as part of this process.
5. If the fabric link fails for the sixth time within an hour, the router permanently shuts down the link.

FEC fabric link system log messages

Lists the syslog messages the router displays for FEC fabric link conditions.

This topic helps you to identify the syslog messages the router displays after retuning a FEC fabric link.

The router displays these syslog messages after retuning:

If the link..	then the router displays this syslog message
is noisy at inception or during bring up	`LC/0/2/CPU0:Jan 13 00:56:03.939 UTC: npu_drvr[128]: %FABRIC-NPU_DRVR-3-NPU_CPA_GEN_ERR_INFO : Link 0/254 has tuned 100 times and failed to come up. FEC bin is filled to 11` The router displays this syslog message after tuning for 100 times
is noisy post bring up, the router permanently shuts down the link	`LC/0/2/CPU0:Jan 13 00:20:16.251 UTC: npu_drvr[128]: %FABRIC-NPU_DRVR-3-NPU_CPA_GEN_ERR_INFO : FEC check failures on link 0/254. FEC bin is filled to 14`

Verify the FEC links

Describes how to verify FEC link information on the router using the **show controllers npu link-info** command and how to interpret the significant fields in the command output.

Procedure

Verify the FEC link information using **show controllers npu link-info** command.

Example

```
Router#show controllers npu link-info rx 254 255 fsm instance 0 location
0/2/CPU0 detail
Sat Jan 13 00:39:49.448 UTC

Node ID: 0/2/CPU0
Link ID: 0/2/0/254    255      Oper State: DOWN   0/FC1/2/158
Event                       State                  Timestamp
+-------------------------------------------------------------------------------+
LINK_UP_INTR                UP                     Sat Jan 13 00:18:44 2018
BAD_FEC_BELOW_THR           PORT_ACTIVATE_DELAYED  Sat Jan 13 00:19:16 2018
LINK_MON                    FAB_PORT_CREATED       Sat Jan 13 00:19:17 2018
LINK_MON                    ACTIVATED              Sat Jan 13 00:19:19 2018
LINK_UP_INTR                MAC_UP                 Sat Jan 13 00:19:24 2018
LINK_UP_INTR                PEER_DISCOVERY         Sat Jan 13 00:19:24 2018
LINK_UP_INTR                PEER_DETECTED          Sat Jan 13 00:19:24 2018
LINK_UP_INTR                TOPOLOGY_CHECK         Sat Jan 13 00:19:24 2018
LINK_UP_INTR                SYNC_WAIT              Sat Jan 13 00:19:24 2018
LINK_UP_INTR                KEEPALIVE_START        Sat Jan 13 00:19:24 2018
LINK_UP_INTR                CHECK_REACH            Sat Jan 13 00:19:24 2018
LINK_UP_INTR                UP                     Sat Jan 13 00:19:24 2018
BAD_FEC                     UP                     Sat Jan 13 00:20:16 2018
DIS_PERM_SHUT               MAC_UP                 Sat Jan 13 00:20:16 2018
DIS_PERM_SHUT               STOPPED                Sat Jan 13 00:20:16 2018
+-------------------------------------------------------------------------------+
```

This table describes the significant fields shown in this example.

Table 15: show controllers npu link-info field descriptions

Field	Description
BAD_FEC_BELOW_THR	There are FEC failures, but the number of failures has not exceeded the predefined threshold (in this case, 5 per hour). The router retunes and checks for FEC improvement.
BAD_FEC	This part of the log entry indicates that FEC detected failures, and the number of these failures surpassed a predefined threshold. As a result, the decision was made to permanently shut down the affected interface or port as a protective measure.
DIS_PERM_SHUT	The link or port has been intentionally disabled and is in a shutdown state after FEC fails for the threshold limit (After fifth failure).

Disable fabric link management for uncorrectable errors

Describes how to disable the fabric link management for uncorrectable errors feature, which is enabled by default on the router.

Fabric link management for uncorrectable errors is enabled by default. To disable this feature, use the **hw-module fabric-fec-monitor disable** command in XR Config mode mode.

Procedure

1. Enter the global configuration mode.

   Example

   ```
   Router# configure
   ```

2. Disable the fabric FEC monitor.

   Example

   ```
   Router(config)# hw-module fabric-fec-monitor disable
   ```

3. Save the changes.

   Example

   ```
   Router(config)# commit
   ```

Fault recovery handling

Describes how the **hw-module fault-recovery** command sets the number of recovery attempts the router makes before permanently shutting down a faulty card.

The **hw-module fault-recovery** command is a configuration feature that

- manages fault recovery attempts for line cards, fabric cards, and route processors, enables administrators to define a specific threshold for recovery attempts before permanent shutdown, and
- replaces the previous time-based reset mechanism to ensure faulty hardware enters a shutdown state after the configured limit.

Table 16: Feature history table

Feature Name	Release Information	Feature Description
Fault recovery handling	Release 26.1.1	Introduced in this release on: Centralized Systems (8400 [ASIC: K100])(select variants only*) * This feature is now supported on Cisco 8404-SYS-D routers.

Feature Name	Release Information	Feature Description
Fault recovery handling	Release 25.4.1	Introduced in this release on: Fixed Systems (8010 [ASIC: A100])(select variants only*) *This feature is supported on: • 8011-32Y8L2H2FH • 8011-12G12X4Y-A/D
Fault recovery handling	Release 25.1.1	Introduced in this release on: Fixed Systems (8700 [ASIC: K100], 8010 [ASIC: A100])(select variants only*) *This feature is supported on: • 8011-4G24Y4H-I • 8712-MOD-M
Fault recovery handling	Release 24.4.1	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100])(select variants only*); Modular Systems (8800 [LC ASIC: P100])(select variants only*) *This feature is supported on: • 8212-48FH-M • 8711-32FH-M • 88-LC1-36EH • 88-LC1-12TH24FH-E • 88-LC1-52Y8H-EM
Fault recovery handling	Release 24.2.11	You can now configure the number of fault recovery attempts by a line card, fabric card or a route processor before it permanently shuts down, thus preventing a faulty card from entering into a cycle of automatic recovery. This feature introduces this change: CLI: • **hw-module fault-recovery** YANG DATA Model: • New XPaths for Cisco-IOS-XR-hw-module-cfg.yang (refer to Github, YANG Data Models Navigator)

In the previous releases, if a line card, fabric card or a route processor experienced a fault, they used to trigger fault recovery and reboot themselves to be operational. Fault recovery mechanism was time based as the fault recovery count used to reset to zero if the card remained operational for more than hour. After the fault recovery count exceeded five, then the faulty card was shut down. As power related faults triggered were not frequent, and fault recovery count used to reset to zero, the card never entered the shut down mode. As a result the card always attempted for fault recovery.

> **Note**
>
> The **hw-module fault-recovery** configuration is not applicable for BMC instance

Configure fault recovery attempts

Describes how to configure the number of fault recovery attempts the router makes on a faulty card before permanently shutting it down.

This task shows how to configure the fault recovery attempts on the fabric card FC0 and how to verify the configuration on the router.

Procedure

1. Enter the global configuration mode.

   Example

   ```
   Router#configure
   ```

2. Configure the fault recovery attempts on the fabric card.

   Example

   ```
   Router (config)#hw-module fault-recovery location 0/FC0 count 1
   ```

3. Save or commit the changes.

   Example

   ```
   Router(config)#commit
   ```

4. Verify the configured fault recovery count. Use the **show running-config formal | include hw-module** command to display the number of times a card can initiate recovery attempts before shutting down.

   Example

   ```
   Router#show running-config formal | include hw-module
   Building configuration...
   hw-module fault-recovery location 0/FC0 count 1
   ```

5. Review the system logs generated when the number of fault recovery attempts on the card exceeds the configured count.

Example

```
Router:Dec 4 15:44:22.950 PST: shelfmgr[121]:
%PLATFORM-SHELFMGR-2-FAULT_ACTION_CARD_SHUTDOWN : Forced shutdown requested
for card 0/FC0. Reason Fault retry attempts exceeded configured count(1)
```

Example

```
Router:Dec 4 15:44:25.247 PST: shelfmgr[121]:
%PLATFORM-SHELFMGR-4-CARD_SHUTDOWN : Shutting down 0/FC0: Fault retry attempts
 exceeded configured count(1)
```

6. Confirm the reason for the card shutdown. Use the **show reboot history** command to get the reason of card shutting down. In this example, it shows that the card was shut down due to **Fault retry attempts exceeded configured count(1)**.

Example

```
Router#show reboot history location 0/FC0 detail
Mon Dec  4 15:44:55.827 PST
-------------------------------------------------------------------------------
No   Attribute       Value
-------------------------------------------------------------------------------
1    Time (PST)      Dec 04 2023 15:44:22
     Cause Code      0x0800000d
     Cause String    REBOOT_CAUSE_FM
     Graceful Reload No
     Kdump Requested No
     Reason          Fault retry attempts exceeded configured count(1)
```

7. Verify the current state of the card that was shut down due to the fault recovery handling feature. Use the **show platform** command to see the current state of the card.

Example

```
Router#show platform
Mon Oct 2 21:08:03.383 UTC

Node               Type                     State                    Config
state
-------------------------------------------------------------------------------
0/RP0/CPU0         8800-RP(Active)          IOS XR RUN               NSHUT
0/RP0/BMC0         8800-RP                  OPERATIONAL               NSHUT
0/RP1/CPU0         8800-RP(Standby)         IOS XR RUN               NSHUT
0/RP1/BMC0         8800-RP                  OPERATIONAL                NSHUT
0/3/CPU0           8800-LC-48H              IOS XR RUN               NSHUT
0/FC0              8812-FC                  SHUT DOWN                NSHUT
0/FC3              8812-FC                  OPERATIONAL              NSHUT
0/FT0              SF-D-12-FAN              OPERATIONAL              NSHUT
0/FT1              SF-D-12-FAN              OPERATIONAL              NSHUT
0/FT2              SF-D-12-FAN              OPERATIONAL              NSHUT
0/FT3              SF-D-12-FAN              OPERATIONAL              NSHUT
0/PT0              FAM7000-ACHV-TRAY        OPERATIONAL              NSHUT
0/PT1              FAM7000-ACHV-TRAY        OPERATIONAL              NSHUT
```

```
0/PT2              FAM7000-ACHV-TRAY        OPERATIONAL               NSHUT
Router#
```

Periodic syslog messages for shutdowns due to fault-recovery failures

Describes the periodic syslog messages the router generates when a card is shut down because of repeated fault-recovery failures, which repeat every 60 minutes until the operator manually recovers the card.

A periodic shutdown syslog message is a log message generated by the router when

- the LC, FC, or RP experiences a fault,
- the Cisco IOS XR software triggers the fault recovery cycle, attempting to reboot the LC, FC, or RP to restore operational status, and
- if the LC, FC, or RP fails to become operational after this recovery attempt, the Cisco IOS XR software proceeds to shut down the affected component and generates a shutdown syslog message immediately after the shutdown.

Table 17: Feature history table

Feature Name	Release Information	Feature Description
Periodic syslog messages for shutdowns due to fault-recovery failures	Release 26.1.1	Introduced in this release on: Centralized Systems (8400 [ASIC: K100]) (select variants only*) *This feature is now supported on the Cisco 8404-SYS-D routers.
Periodic syslog messages for shutdowns due to fault-recovery failures	Release 25.4.1	Introduced in this release on: Fixed Systems (8010 [ASIC: A100])(select variants only*) *This feature is supported on: • 8011-32Y8L2H2FH • 8011-12G12X4Y-A/D
Periodic syslog messages for shutdowns due to fault-recovery failures	Release 25.1.1	Introduced in this release on: Fixed Systems (8700 [ASIC: K100], 8010 [ASIC: A100])(select variants only*) *This feature is supported on: • 8712-MOD-M • 8011-4G24Y4H-I

Feature Name	Release Information	Feature Description
Periodic syslog messages for shutdowns due to fault-recovery failures	Release 24.4.1	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100])(select variants only*); Centralized Systems (8600); Modular Systems (8800 [LC ASIC: Q100, Q200, P100])(select variants only*) Cisco IOS XR Software now generates a syslog message immediately to indicate its shutdown state after a Line Card (LC), Fabric Card (FC), or Route Processor (RP) shuts down due to fault-recovery failure. This syslog message is repeated every 60 minutes to keep you informed of the shutdown status. This enhancement helps in identifying and troubleshooting shutdown LC, FC, or RP components. *This feature is now supported on: • 8212-48FH-M • 8711-32FH-M • 88-LC1-12TH24FH-E • 88-LC1-36EH • 88-LC1-52Y8H-EM

By default, the Cisco IOS XR software performs the fault recovery cycle five times before shutting down the LC, FC, or RP. If the fault recovery handling count is configured, the Cisco IOS XR software shuts down the LC, FC, or RP after the expiry of the fault recovery count. For more information, refer to Fault recovery handling on page 70.

Before Release 24.4.1, the Cisco IOS XR software generates a shutdown syslog message only once immediately after the LC, FC, or RP shut down to notify you of the shutdown.

From Release 24.4.1 onwards, the Cisco IOS XR software generates this shutdown syslog message immediately after the LC, FC, or RP shuts down and repeats the shutdown syslog message every 60 minutes to notify you of the shutdown until you manually shut down the LC, FC, or RP using the **hw-module shutdown location** or **reload location** commands.

```
Router: Dec 4 15:44:22.950 PST: shelfmgr[121]:
%PLATFORM-SHELFMGR-2-FAULT_ACTION_CARD_SHUTDOWN : Forced shutdown requested
for card 0/FC0. Reason Fault retry attempts exceeded configured count(1)
Router:Dec 4 15:44:25.247 PST: shelfmgr[121]: %PLATFORM-SHELFMGR-4-CARD_SHUTDOWN
 : Shutting down 0/FC0: Fault retry attempts exceeded configured count(1)
```

Limitations and restrictions for periodic shutdown syslog messages

This topic lists the restrictions that the system generates for periodic shutdown syslog messages.

When you manually shut down a specific node using the **shutdown location** command in XR EXEC mode or the **hw-module shutdown location** command in XR Config mode, the Cisco IOS XR software doesn't generate the shutdown syslog messages.

Machine check error notifications

Describes how the router logs machine check errors to the MCE log file and emits syslog messages with error details so that an operator can identify and act on hardware-detected processor faults.

The Machine Check Error (MCE) is a hardware error detection mechanism that

- identifies hardware failures in CPUs, memory, power, or other critical components
- triggers system logs in `/var/log/mcelog.log` to record the event, and
- initiates corrective actions such as restarting affected line cards, route processors, or the entire router.

Before Release 24.4.1, you must manually check the MCE error logs in the location `/var/log/mcelog.log` or on the syslog server to determine whether the router reboot was due to a MCE or another issue.

From Release 24.4.1 onwards, the Cisco IOS XR Software logs the error in the MCE log file and notifies you by displaying a syslog message.

This is an example of an MCE that the router displays:

```
Router:Oct 28 22:37:44.293 UTC: shelfmgr[377]:
%PLATFORM-CPA_INTF_SHELFMGR-3-CPU_MCERR : CPU Machine Check Error
condition reported for node0_RP0_CPU0: corrected DIMM memory error count
exceeded threshold: 10 in 24h . Reported at 2024-10-28 22:37:44.00000 UTC
```

Table 18: Feature history table

Feature Name	Release Information	Feature Description
Machine check error notifications	Release 26.1.1	Introduced in this release on: Centralized Systems (8400 [ASIC: K100])(select variants only*) * This feature is now supported on Cisco 8404-SYS-D routers.
Machine check error notifications	Release 25.4.1	Introduced in this release on: Fixed Systems (8010 [ASIC: A100])(select variants only*) *This feature is supported on: • 8011-32Y8L2H2FH • 8011-12G12X4Y-A/D
Machine check error notifications	Release 25.1.1	Introduced in this release on: Fixed Systems (8700 [ASIC: K100], 8010 [ASIC: A100])(select variants only*) *This feature is supported on: • 8712-MOD-M • 8011-4G24Y4H-I

Feature Name	Release Information	Feature Description
Machine check error notifications	Release 24.4.1	Introduced in this release on: Fixed Systems (8200, 8700); Centralized Systems (8600); Modular Systems (8800 [LC ASIC: Q100, Q200, P100]) You can now identify and resolve MCE-related issues quickly and easily because Cisco IOS XR Software displays a syslog notification for MCE errors, eliminating the need to manually check for them in the MCE log file.

Syslog message information

The syslog message displays this information about the error:

- Error title - CPA_INTF_SHELFMGR-3-CPU_MCERR
- Error description - CPU Machine Check Error
- Error location - RP/0/RP0/CPU0
- Error type - DIMM memory error
- Error time - 2024-10-28 22:37:44.00000 UTC

Error detail and recommended action

- Cisco feature navigator error messages tool - Provides detailed error information and recommended actions. For more information, refer to View error details in the Cisco Feature Navigator error messages tool on page 78.
- MCE log file - Stores all past errors in the MCE log file located at `/var/log/mcelog.log`. You can determine if the current error has occurred in the past using the MCE log file and troubleshoot accordingly. For more information, refer to View error details in the MCE log file on page 78

MCE major errors in a router

These are some of the MCE major errors that occurs in a router:

- Card power zone error: Displays under voltage or over voltage failure condition on the Line Card (LC) or Fabric Card (FC). During such an error, the system will attempt to recover by power-cycling the LC or FC.
- Single Event Upset (SEU) error: Displays corrected and uncorrected SEU events that can happen in FPGA devices.
- Central Processing Unit (CPU) error: Displays all CPU errors.

If these errors occur in a router, you can see the occurrence of these errors using the **show alarms** command. For more information, refer to Monitoring Alarms and Implementing Alarm Log Correlation section in the *System Monitoring Configuration Guide for Cisco 8000 Series Routers*.

Restrictions for MCE major errors

Notes that from Cisco IOS XR Release 24.2.11 onward, the show alarm command output includes only the power zone errors for machine check error major events.

From Release 24.2.11, **show alarm** command output includes only the power zone errors.

View error details in the Cisco Feature Navigator error messages tool

Describes how to view machine check error details in the Cisco Feature Navigator error messages tool by searching by release, error title, or comparing different Cisco IOS XR releases.

Perform these steps to see error details in the cisco feature navigator error messages tool:

Procedure

1. Login to Cisco Feature Navigator Error Messages Tool. The cisco feature navigator error messages tool provides these search options:
   - Release - Displays error details based on specific Cisco IOS XR Release.
   - Error - Displays the error details based on the provided error title.
   - Compare - Displays the error details by comparing different Cisco IOS XR Releases.
2. Click on **Error** option.
3. Enter the error title, for example, CPA_INTF_SHELFMGR-3-CPU_MCERR.
4. Click **Submit** to view the error details.

   The error details contain these sections:
   - Error
   - Severity
   - Limit
   - Format
   - Explanation
   - Recommended action

   For more information about error details sections and Cisco Feature Navigator Error Messages Tool, refer to Cisco IOS XR System Error Message Reference Guide.

View error details in the MCE log file

Describes how to view machine check error details by opening the MCE log file at `/var/log/mcelog.log` on the router.

Perform these steps to see error details in the MCE log file:

Procedure

1. Navigate to MCE log file located at `/var/log/mcelog.log`.
2. Open **mcelog.log** file to view the error details.

7 Storage media sanitization

Topics:

- Storage media sanitization
- Secure erase of router SSD data
- Storage media sanitization
- Exclude Sensitive Information in Show Running Configurations Output

Describes the storage media sanitization features on Cisco 8000 Series Routers, including factory reset, secure erase, and sanitization of sensitive information in the show running-configuration output.

Refer to this chapter to understand the storage media sanitization features available on Cisco 8000 Series Routers and the procedures used to erase or mask sensitive data on the router.

Storage media sanitization

Describes how the router erases sensitive data, configurations, and keys from a route processor or line cards.

Storage media sanitization is a data erasing or data clearing mechanism that

- erases customer-sensitive data from Route Processors (RPs) or line cards
- prepares hardware for Return Merchandise Authorization (RMA) or off-site shipping, and
- allows hardware to remain in the slot without requiring immediate intervention from on-site personnel.

Table 19: Feature history table

Feature Name	Release Information	Feature Description
Storage Media Sanitization	Release 7.3.4	To comply with NIST SP 800-88 guidelines for Media Sanitization, it is important that your organization ensures that no easily reconstructible data is stored in the router and associated devices after it has left the control of your organization or is no longer protected by confidentiality categorization. With this feature, you can erase and overwrite any sensitive data, configuration, or keys present in the route processor or line card, ensuring media sanitization and preventing unauthorized data retrieval.

When you identify an RP or line card for RMA, or you require to ship it outside your organization, a service personnel may not be available on-site to remove the card immediately. However, you can reset your RP or line card to erase customer-sensitive data and let the RP or line card remain in the slot. The RP or line card shuts down automatically after the factory reset is complete.

Secure erase of router SSD data

Describes the secure erase data security feature that removes all customer-sensitive data, configurations, and keys from the solid state drive on a line card, route processor, or the entire router in compliance with NIST 800-88 guidelines and then shuts the node down.

Secure erase is a data security feature that:

- securely erases solid-state drive (SSD) data on a particular node or the entire router, and
- removes all customer-sensitive data, configurations, and keys from the storage device (SSD) in compliance with National Institute for Standards and Technology (NIST) 800-88 guidelines for media sanitization.

The secure erase feature is ideal for scenarios where the router is to be decommissioned. It is also useful when the data needs to be completely removed for security reasons.

Table 20: Feature history table

Feature Name	Release Information	Feature Description
Secure erase of router SSD data		Introduced in this release on: Centralized Systems (8400 [ASIC: K100])(select variants only*) *This feature is now supported on the Cisco 8404-SYS-D router.
Secure erase of router SSD data	Release 25.1.1	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200, P100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC:Q200]); Modular Systems (8800 [LC ASIC: Q100, Q200, P100]) You can now efficiently and securely manage the data and configuration settings on your routers by ensuring complete removal of sensitive data from the routers that are to be decommissioned, or for security purposes. This feature securely erases the solid state drive (SSD) data on a particular card such as a line card or a route processor, or on the entire router and shuts it down. The feature introduces these changes: CLI: • **secure-erase** YANG Data Model: • `Cisco-IOS-XR-secure-erase-act`

Benefits of secure erase functionality

The secure erase functionality on Cisco IOS XR routers provides these benefits:

- Complete data removal from the device for security purposes
- Suitable for device decommissioning or re-purposing
- Can be applied to individual nodes or to the entire router

Restriction for secure erase functionality

Refer to this topic to understand the restrictions that apply to the secure erase functionality on Cisco IOS XR routers.

Secure erase functionality on routers is subjected to a restriction that you cannot initiate it if the entire system is down or if no active RP is booted to IOS XR OS.

Perform secure erase on a router

Describes how to initiate the secure-erase operation on a specified location from the router CLI and how to confirm completion by reviewing the disk erase syslog messages.

Before you begin

- Ensure the active RP is operational to initiate the secure erase process.
- Ensure that there is no immediate requirement for the router after the secure erase process, since it involves complete data removal and shutdown of the router.
- Keep a backup of the router data as a precautionary measure.

Procedure

1. Initiate secure erase process on the router CLI.

   Example

```
Router#secure-erase location 0/RP1/CPU0
Tue Mar 11 11:17:51.294 UTC
Performing secure erase operation will erase the SSD and shut down the card.
 Proceed?
[confirm]
```

2. Check system logs to confirm that the secure erase process is completed.

   Example

```
RP/0/RP0/CPU0:Mar 11 11:28:55.862 UTC: shelfmgr[159]:
%PLATFORM-CPA_INTF_SHELFMGR-4-CARD_REIMAGE_CFG_DONE : Successfully configured
 card 0/RP1/CPU0 for reimage operation, boot mode: IPXE_INTERNAL
RP/0/RP0/CPU0:Mar 11 11:31:08.610 UTC: shelfmgr[159]:
%PLATFORM-SHELFMGR-4-DISK_ERASE_START : Started disk erase operation on
0/RP1/CPU0
RP/0/RP0/CPU0:Mar 11 11:31:10.455 UTC: shelfmgr[159]:
%PLATFORM-SHELFMGR-4-DISK_ERASE_IN_PROGRESS : [bash(1119)] Performing NIST
recommended purge sanitization method on /dev/nvme0n1 on 0/RP1/CPU0
RP/0/RP0/CPU0:Mar 11 11:52:12.890 UTC: shelfmgr[159]:
%PLATFORM-SHELFMGR-4-DISK_ERASE_DONE : Disk erase operation finished
successfully on 0/RP1/CPU0
RP/0/RP0/CPU0:Mar 11 11:52:18.553 UTC: shelfmgr[159]:
%PLATFORM-SHELFMGR-6-INFO_LOG : 0/RP1/CPU0 is shutdown
```

Storage media sanitization

Describes how the router erases sensitive data, configurations, and keys from a route processor or line cards.

Storage media sanitization is a data erasing or data clearing mechanism that

- erases customer-sensitive data from Route Processors (RPs) or line cards
- prepares hardware for Return Merchandise Authorization (RMA) or off-site shipping, and
- allows hardware to remain in the slot without requiring immediate intervention from on-site personnel.

Table 21: Feature history table

Feature Name	Release Information	Feature Description
Storage Media Sanitization	Release 7.3.4	To comply with NIST SP 800-88 guidelines for Media Sanitization, it is important that your organization ensures that no easily reconstructible data is stored in the router and associated devices after it has left the control of your organization or is no longer protected by confidentiality categorization. With this feature, you can erase and overwrite any sensitive data, configuration, or keys present in the route processor or line card, ensuring media sanitization and preventing unauthorized data retrieval.

When you identify an RP or line card for RMA, or you require to ship it outside your organization, a service personnel may not be available on-site to remove the card immediately. However, you can reset your RP or line card to erase customer-sensitive data and let the RP or line card remain in the slot. The RP or line card shuts down automatically after the factory reset is complete.

Exclude Sensitive Information in Show Running Configurations Output

Describes how to mask sensitive information such as strings, usernames, passwords, comments, and IP addresses in the **show running-configuration** command output by enabling sanitization on the nonvolatile generation (NVGEN) process.

The configuration output sanitization is a security feature that

- masks sensitive information within the running configuration output
- replaces sensitive strings with a placeholder, and
- protects sensitive data such as passwords and IP addresses from unauthorized exposure.

Table 22: Feature History Table

Feature Name	Release Information	Feature Description
Excluding Sensitive Information in Show Running Configurations Command Output	Release 7.5.4	You can now exclude sensitive information such as strings, usernames, passwords, comments, or IP addresses within the **show running-configuration** command output by enabling sanitization on the nonvolatile generation (NVGEN) process. With this feature, you can achieve better data protection to prevent cybersecurity risks compared to regular router algorithms. This feature introduces the **nvgen default-sanitize** command.

The **show running configuration** command uses the nonvolatile generation (NVGEN) process in Cisco IOS-XR software to collect configuration information from every system component and construct a running configuration file. Because this file often contains sensitive information that poses a security threat, this feature provides a mechanism to sanitize the output. When you enable sanitization, the NVGEN process replaces the corresponding information with the `<removed>` string to prevent unauthorized access to critical data.

The feature allows you to mask these types of sensitive information in the show running configuration output:

- Strings
- Usernames
- Passwords
- Comments
- IP Addresses

On enabling the sanitization in show running configurations, the NVGEN process replaces the corresponding information with **<removed>** string. For example, if you enable sanitization for IP Addresses, the show running configuration includes the **<removed>** string in place of all the IP Addresses in the output.

This feature introduces the **nvgen default-sanitize** command.

Configure sanitization

Use these tasks to configure sanitization for each category of sensitive information:

- Sanitize strings
- Sanitize usernames
- Sanitize passwords
- Sanitize comments
- Sanitize IP addresses

Sanitize strings

Describes how to mask configurable strings, such as interface descriptions, in the **show running-configuration** command output by enabling the **strings** category of the NVGEN default-sanitize feature.

When you enable sanitization for the **strings** category, the NVGEN process replaces configurable string values, such as interface descriptions, with the **<removed>** token in the **show running-configuration** output.

Procedure

1. Enter the global configuration mode.

   Example

   ```
   Router# config
   ```

2. Enable default sanitization for strings.

   Example

   ```
   Router:(config)# nvgen default-sanitize strings
   ```

3. Commit the changes.

   Example

   ```
   Router:(config)# commit
   ```

4. Verify that string sanitization is enabled in the running configuration.

   Example

   ```
   Router# show run nvgen
   nvgen
    default-sanitize strings
   !
   ```

5. Verify that configurable strings are masked in the interface running configuration.

   Example

   ```
   Router# show run int Hu0/2/0/4
   interface HundredGigE0/2/0/4
    ! This is comment 1
    description <removed>
    !
   ```

Sanitize usernames

Describes how to mask configured usernames in the **show running-configuration** command output by enabling the **usernames** category of the NVGEN default-sanitize feature.

When you enable sanitization for the **usernames** category, the NVGEN process replaces configured usernames with the **<removed>** token in the **show running-configuration** output.

Procedure

1. Enter the global configuration mode.

   Example

   ```
   Router# config
   ```

2. Enable default sanitization for usernames.

   Example

   ```
   Router:(config)# nvgen default-sanitize usernames
   ```

3. Commit the changes.

   Example

   ```
   Router:(config)# commit
   ```

4. Verify that username sanitization is enabled in the running configuration.

   Example

   ```
   Router# show run nvgen
   nvgen
    default-sanitize usernames
   !
   ```

5. Verify that usernames are masked in the user running configuration.

   Example

   ```
   Router# show run username test
   username <removed>
    group root-lr
    password 7 172864HJWBJHBCWH
   !
   ```

Sanitize passwords

Describes how to mask configured passwords in the **show running-configuration** command output by enabling the **passwords** category of the NVGEN default-sanitize feature.

When you enable sanitization for the **passwords** category, the NVGEN process replaces password values with the **<removed>** token in the **show running-configuration** output.

Procedure

1. Enter the global configuration mode.

   Example

   ```
   Router# config
   ```

2. Enable default sanitization for passwords.

   Example

   ```
   Router:(config)# nvgen default-sanitize passwords
   ```

3. Commit the changes.

   Example

   ```
   Router:(config)# commit
   ```

4. Verify that password sanitization is enabled in the running configuration.

   Example

   ```
   Router# show run nvgen
   nvgen
    default-sanitize passwords
   !
   ```

5. Verify that passwords are masked in the user running configuration.

   Example

   ```
   Router# show run username test
   username test
    group root-lr
    password 7 <removed>
   !
   ```

Sanitize comments

Describes how to mask configuration comments in the **show running-configuration** command output by enabling the **comments** category of the NVGEN default-sanitize feature.

When you enable sanitization for the **comments** category, the NVGEN process replaces inline configuration comments with the **<comments removed>** token in the **show running-configuration** output.

Procedure

1. Enter the global configuration mode.

Example

```
Router# config
```

2. Enable default sanitization for comments.

Example

```
Router:(config)# nvgen default-sanitize comments
```

3. Commit the changes.

Example

```
Router:(config)# commit
```

4. Verify that comment sanitization is enabled in the running configuration.

Example

```
Router# show run nvgen
nvgen
 default-sanitize comments
!
```

5. Verify that comments are masked in the interface running configuration.

Example

```
Router# show run int Hu0/2/0/4
interface HundredGigE0/2/0/4
 ! <comments removed>
 description This is bundle member
 !
```

Sanitize IP addresses

Describes how to mask IPv4 addresses in the **show running-configuration** command output by enabling the **ipaddrs** category of the NVGEN default-sanitize feature.

When you enable sanitization for the **ipaddrs** category, the NVGEN process replaces IP address values with the **<removed>** token in the **show running-configuration** output.

Procedure

1. Enter the global configuration mode.

Example

```
Router# config
```

2. Enable default sanitization for IP addresses.

Example

```
Router:(config)# nvgen default-sanitize ipaddrs
```

3. Commit the changes.

Example

```
Router:(config)# commit
```

4. Verify that IP addresses are masked in the interface running configuration.

Example

```
Router# show run int Hu0/2/0/4
interface HundredGigE0/2/0/4
 ! This is comment 1
 description This is bundle member
  ipv4 address <removed> <removed>
!
```