



Product Overview

This chapter consists of these sections:

- [Supervisor Engine Memory Devices and Ports, page 1-1](#)
- [User Interfaces, page 1-5](#)
- [Module Status Monitoring, page 1-6](#)
- [Software Features Supported in Hardware by the PFC and DFC, page 1-6](#)



Tip

For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

[Participate in the Technical Documentation Ideas forum](#)

Supervisor Engine Memory Devices and Ports

For complete information about the chassis, modules, and software features supported by Cisco IOS Release 12.2SX, see the *Release Notes for Cisco IOS Release 12.2SX*:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/release/notes/ol_14271.html

These sections describe the ports and flash memory devices on the supervisor engines:

- [Understanding Supervisor Engine 720-10GE Memory Devices and Ports, page 1-1](#)
- [Understanding Supervisor Engine 720 Memory Devices and Ports, page 1-2](#)
- [Understanding Supervisor Engine 32 Memory Devices and Ports, page 1-4](#)
- [Understanding ME6500 Flash Memory Devices and Ports, page 1-5](#)

Understanding Supervisor Engine 720-10GE Memory Devices and Ports

These sections describe the Supervisor Engine 720-10GE memory devices and ports:

- [Supervisor Engine 720-10GE Flash Memory Devices, page 1-2](#)
- [Supervisor Engine 720-10GE Ports, page 1-2](#)

Supervisor Engine 720-10GE Flash Memory Devices

The Supervisor Engine 720-10GE has these flash memory devices:

- **disk0:** (active) and **slavedisk0:** (standby):
 - External CompactFlash Type II slots
 - For CompactFlash Type II flash PC cards sold by Cisco Systems, Inc.
- **sup-bootdisk:** (active) and **slavesup-bootdisk:** (standby):
 - Switch processor (SP) 1-GB internal CompactFlash flash memory
 - From SP ROMMON, it is **bootdisk:**
 - Not accessible from route processor (RP) ROMMON
- **bootflash:** (active) and **slave-bootflash:** (standby):
 - RP 64-MB internal flash memory
 - Not accessible from SP ROMMON

Supervisor Engine 720-10GE Ports

The Supervisor Engine 720-10GE has these ports:

- Console port—EIA/TIA-232 (RS-232) port
- Ports 1 and 2
 - Gigabit Ethernet SFP (fiber or 10/100/1000 Mbps RJ-45)
 - Fast Ethernet SFP
- Port 3—10/100/1000 Mbps RJ-45
- Ports 4 and 5—10-Gigabit Ethernet X2



Note

The 1-Gigabit Ethernet ports and the 10-Gigabit Ethernet ports have the same QoS port architecture (2q4t/1p3q4t) unless you disable the 1-Gigabit Ethernet ports with the **mls qos 10g-only** global configuration command. With the 1-Gigabit Ethernet ports disabled, the QoS port architecture of the 10-Gigabit Ethernet ports is 8q4t/1p7q4t.

See the “[Configuring Optional Interface Features](#)” section on [page 8-6](#) for information about configuring the ports.

Understanding Supervisor Engine 720 Memory Devices and Ports

These sections describe the Supervisor Engine 720 memory devices and ports:

- [Supervisor Engine 720 Flash Memory Devices, page 1-3](#)
- [Configuring Supervisor Engine 720 Ports, page 1-3](#)

Supervisor Engine 720 Flash Memory Devices

The Supervisor Engine 720 has these flash memory devices:

- **disk0:** and **disk1:** (active) and **slavedisk0:** and **slavedisk1:** (standby):
 - External CompactFlash Type II slots
 - For CompactFlash Type II flash PC cards sold by Cisco Systems, Inc.
- **sup-bootflash:** (active) and **slavesup-bootflash:** (standby):
 - Switch processor (SP) 64-MB internal flash memory
 - From SP ROMMON, it is **bootflash:**
 - Not accessible from route processor (RP) ROMMON
- With WS-CF-UPG=, **sup-bootdisk:** (active) and **slavesup-bootflash:** (standby):
 - SP 512-MB internal CompactFlash flash memory
 - From SP ROMMON, it is **bootdisk:**
 - Not accessible from RP ROMMON
 - See this publication for more information:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_17277.html
- **bootflash:** (active) and **slave-bootflash:** (standby):
 - RP 64-MB internal flash memory
 - Not accessible from SP ROMMON

Configuring Supervisor Engine 720 Ports

The Supervisor Engine 720 has these ports:

- Port 1—Small form-factor pluggable (SFP); no unique configuration options.
- Port 2—RJ-45 connector and an SFP connector (default). To use the RJ-45 connector, you must change the configuration.

To configure port 2 on a Supervisor Engine 720 to use either the RJ-45 connector or the SFP connector, perform this task:

	Command	Purpose
Step 1	Router(config)# interface gigabitethernet slot/2	Selects the Ethernet port to be configured.
Step 2	Router(config-if)# media-type {rj45 sfp}	Selects the connector to use.

This example shows how to configure port 2 on a Supervisor Engine 720 in slot 5 to use the RJ-45 connector:

```
Router(config)# interface gigabitethernet 5/2
Router(config-if)# media-type rj45
```

See the “Configuring Optional Interface Features” section on page 8-6 for more information about configuring the ports.

Understanding Supervisor Engine 32 Memory Devices and Ports

These sections describe the Supervisor Engine 32 memory devices and ports:

- [Supervisor Engine 32 Flash Memory Devices, page 1-4](#)
- [Supervisor Engine 32 Ports, page 1-4](#)

**Note**

Supervisor Engine 32 does not support switch fabric connectivity.

Supervisor Engine 32 Flash Memory Devices

The Supervisor Engine 32 has these flash memory devices:

- **disk0:** (active) and **slavedisk0:** (standby):
 - External CompactFlash Type II slots
 - For CompactFlash Type II flash PC cards sold by Cisco Systems, Inc.
- **sup-bootdisk:** (active) and **slavesup-bootflash:** (standby):
 - Switch processor (SP) 256-MB internal CompactFlash flash memory
 - From SP ROMMON, it is **bootdisk:**
 - Not accessible from route processor (RP) ROMMON
- **bootflash:** (active) and **slave-bootflash:** (standby):
 - RP 64-MB internal flash memory
 - Not accessible from SP ROMMON

Supervisor Engine 32 Ports

The Supervisor Engine 32 has these ports:

- Console port—EIA/TIA-232 (RS-232) port
- Two Universal Serial Bus (USB) 2.0 ports—Not currently enabled
- WS-SUP32-GE-3B:
 - Ports 1 through 8—Small form-factor pluggable (SFP)
 - Port 9—10/100/1000 Mbps RJ-45
- WS-SUP32-10GE:
 - Ports 1 and 2—10-Gigabit Ethernet XENPAK
 - Port 3—10/100/1000 Mbps RJ-45

See the [“Configuring Optional Interface Features” section on page 8-6](#) for information about configuring the ports.

Understanding ME6500 Flash Memory Devices and Ports

These sections describe the Cisco ME6500 series Ethernet switch memory devices and ports:

- [ME6500 Flash Memory Devices, page 1-5](#)
- [ME6500 Ports, page 1-5](#)

ME6500 Flash Memory Devices

The ME6500 has these flash memory devices:

- **disk0:**
 - One external CompactFlash Type II slot
 - Supports CompactFlash Type II flash PC cards
- **sup-bootflash:**
 - Switch processor (SP) 128 MB internal CompactFlash flash memory
 - From SP ROMMON, it is **bootflash:**
 - Not accessible from route processor (RP) ROMMON
- **bootflash:**
 - RP 64-MB internal flash memory
 - Not accessible from SP ROMMON

ME6500 Ports

The ME6500 has these ports:

- ME-C6524GS-8S and ME-C6524GT-8S
 - Ports 25–32: Gigabit Ethernet SFP
 - Requires Gigabit Ethernet SFPs
- ME-C6524GS-8S
 - Ports 1–24: Gigabit Ethernet SFP
 - Requires Gigabit Ethernet SFPs
- ME-C6524GT-8S—Ports 1–24: 10/100/1000 Mbps RJ-45 Ethernet ports

User Interfaces

Release 12.2SX supports configuration using the following interfaces:

- CLI—See [Chapter 2, “Command-Line Interfaces.”](#)
- SNMP—See the Release 12.2 IOS *Configuration Fundamentals Configuration Guide* and *Command Reference* at this URL:
http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/ffun_c.html

- Cisco IOS web browser interface—See “Using the Cisco Web Browser” in the *IOS Configuration Fundamentals Configuration Guide* at this URL:
http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf005.html

Module Status Monitoring

The supervisor engine polls the installed modules with Switch Communication Protocol (SCP) messages to monitor module status.

The SCP sends a message every two seconds to each module. Module nonresponse after 3 messages (6 seconds) is classified as a failure. CPU_MONITOR system messages are sent every 30 seconds. After 25 sequential failures (150 seconds), the supervisor engine power cycles the module and sends a CPU_MONITOR TIMED_OUT system message and OIR PWRCYCLE system messages.

Software Features Supported in Hardware by the PFC and DFC

The PFC3 and DFC3 provide hardware support for these Cisco IOS software features:

- Access Control Lists (ACLs) for Layer 3 ports and VLAN interfaces:
 - Permit and deny actions of input and output standard and extended ACLs



Note Flows that require ACL logging are processed in software on the route processor (RP).

- Except on MPLS interfaces, reflexive ACL flows after the first packet in a session is processed in software on the RP
- Dynamic ACL flows



Note Idle timeout is processed in software on the RP.

For more information about PFC and DFC support for ACLs, see [Chapter 49, “Understanding Cisco IOS ACL Support.”](#)

For complete information about configuring ACLs, see the Cisco IOS Security Configuration Guide, Release 12.2, “Traffic Filtering and Firewalls,” at this URL:

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfacls.html

- Bidirectional Protocol Independent Multicast (PIM) in hardware—See “[Understanding IPv4 Bidirectional PIM](#)” section on page 37-9.
- IPv4 Multicast over point-to-point generic route encapsulation (GRE) Tunnels—See the publication at this URL:
http://www.cisco.com/en/US/docs/ios/12_2/interface/configuration/guide/icflogin.html
- Multiple-path Unicast Reverse Path Forwarding (RPF) Check—To configure Unicast RPF Check, see the “[Configuring Unicast Reverse Path Forwarding Check](#)” section on page 47-2.
- Except on MPLS interfaces, Network Address Translation (NAT) for IPv4 unicast and multicast traffic.

Note the following information about hardware-assisted NAT:

- NAT of UDP traffic is not supported in PFC3A mode.
- The PFC3 does not support NAT of multicast traffic.
- The PFC3 does not support NAT configured with a route-map that specifies length.
- When you configure NAT and NDE on an interface, the PFC3 sends all traffic in fragmented packets to the RP to be processed in software. (CSCdz51590)

To configure NAT, see the *Cisco IOS IP Configuration Guide*, Release 12.2, “IP Addressing and Services,” “Configuring IP Addressing,” “Configuring Network Address Translation,” at this URL:

http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfipadr.html

To prevent a significant volume of NAT traffic from being sent to the RP, due to either a DoS attack or a misconfiguration, enter the **mls rate-limit unicast acl {ingress | egress}** command described at this URL:

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_m2.html#mls_rate-limit_unicast_acl

(CSCea23296)

- NetFlow Aggregation—See this URL:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/netflow.html#NetFlow_Aggregation

- Policy-based routing (PBR) for route-map sequences that use the **match ip address**, **set ip next-hop**, and **ip default next-hop** PBR keywords.

To configure PBR, see the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2, “Classification,” “Configuring Policy-Based Routing,” at this URL:

http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfpbr_ps1835_TSD_Products_Configuration_Guide_Chapter.html



Note

If the RP address falls within the range of a PBR ACL, traffic addressed to the RP is policy routed in hardware instead of being forwarded to the RP. To prevent policy routing of traffic addressed to the RP, configure PBR ACLs to deny traffic addressed to the RP.

- Except on MPLS interfaces, TCP intercept—To configure TCP intercept, see the “[Configuring TCP Intercept](#)” section on page 47-2.



Note

The PFC3 does not provide hardware acceleration for tunnels configured with the **tunnel key** command.

- GRE Tunneling and IP in IP Tunneling—The PFC3 and DFC3s support the following **tunnel** commands:
 - **tunnel destination**
 - **tunnel mode gre**
 - **tunnel mode ipip**
 - **tunnel source**
 - **tunnel ttl**
 - **tunnel tos**

Other supported types of tunneling run in software on the RP.

The **tunnel ttl** command (default 255) sets the TTL of encapsulated packets.

The **tunnel tos** command, if present, sets the ToS byte of a packet when it is encapsulated. If the **tunnel tos** command is not present and QoS is not enabled, the ToS byte of a packet sets the ToS byte of the packet when it is encapsulated. If the **tunnel tos** command is not present and QoS is enabled, the ToS byte of a packet as modified by PFC QoS sets the ToS byte of the packet when it is encapsulated.

To configure GRE Tunneling and IP in IP Tunneling, see these publications:

http://www.cisco.com/en/US/docs/ios/12_2/interface/configuration/guide/icflogin.html

http://www.cisco.com/en/US/docs/ios/12_2/interface/command/reference/irfshoip.html

To configure the **tunnel tos** and **tunnel ttl** commands, see this publication for more information:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/12s_tos.html

Note the following information about tunnels:

- Each hardware-assisted tunnel must have a unique source. Hardware-assisted tunnels cannot share a source even if the destinations are different. Use secondary addresses on loopback interfaces or create multiple loopback interfaces. Failure to use unique source addresses may result in control plane failures when software path congestion occurs. (CSCdy72539)
- Each tunnel interface uses one internal VLAN.
- Each tunnel interface uses one additional router MAC address entry per router MAC address.
- The PFC3A does not support any PFC QoS features on tunnel interfaces.
- Other PFC versions support PFC QoS features on tunnel interfaces.
- The RP supports tunnels configured with egress features on the tunnel interface. Examples of egress features are output Cisco IOS ACLs, NAT (for inside to outside translation), TCP intercept, and encryption.
- VLAN ACLs (VACLs)—To configure VACLs, see [Chapter 51, “Configuring Port ACLs and VLAN ACLs.”](#)