Product Overview

This chapter consists of these sections:

Tip For additional information (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/routers/ps368/tsd_products_support_series_home.html

Supported Hardware and Software

For complete information about the chassis, modules, and software features supported by the Cisco 7600 series routers, refer to the *Release Notes for Cisco IOS Release 12.2SX on the Supervisor Engine 720, Supervisor Engine 32, and Supervisor Engine 2*.

User Interfaces

Release 12.2SX supports configuration using the following interfaces:

- CLI—See Chapter 2, "Command-Line Interfaces."
- SNMP—Refer to 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—Refer to "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
- Embedded CiscoView—See the "Configuring Embedded CiscoView Support" section on page 1-2.

Configuring Embedded CiscoView Support

These sections describe configuring Embedded CiscoView support:

- Understanding Embedded CiscoView, page 1-2
- Installing and Configuring Embedded CiscoView, page 1-2
- Displaying Embedded CiscoView Information, page 1-3

Understanding Embedded CiscoView

The Embedded CiscoView network management system is a web-based interface that uses HTTP and SNMP to provide a graphical representation of the router and to provide a GUI-based management and configuration interface.

Installing and Configuring Embedded CiscoView

To install and configure Embedded CiscoView, perform this task:

	Command	Purpose
Step 1	Router# **dir** *device_name*	Displays the contents of the device. If you are installing Embedded CiscoView for the first time, or if the CiscoView directory is empty, skip to Step 4.
Step 2	Router# **delete** *device_name*:**cv/***	Removes existing files from the CiscoView directory.
Step 3	Router# **squeeze** *device_name*:	Recovers the space in the file system.
Step 4	Router# **archive tar /xtract tftp://** *ip_address_of_tftp_server*/**ciscoview.tar** *device_name*:**cv**	Extracts the CiscoView files from the tar file on the TFTP server to the CiscoView directory.
Step 5	Router# **dir** *device_name*:	Displays the contents of the device. In a redundant configuration, repeat Step 1 through Step 5 for the file system on the redundant supervisor engine.
Step 6	Router# **configure terminal**	Enters global configuration mode.
Step 7	Router(config)# **ip http server**	Enables the HTTP web server.
Step 8	Router(config)# **snmp-server community** *string* **ro**	Configures the SNMP password for read-only operation.
Step 9	Router(config)# **snmp-server community** *string* **rw**	Configures the SNMP password for read/write operation.

Note The default password for accessing the router web page is the enable-level password of the router.

For more information about web access to the router, refer to "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

Displaying Embedded CiscoView Information

To display the Embedded CiscoView information, enter the following EXEC commands:

Command	Purpose
Router# **show ciscoview package**	Displays information about the Embedded CiscoView files.
Router# **show ciscoview version**	Displays the Embedded CiscoView version.

Software Features Supported in Hardware by the PFC and DFC

These sections describe the hardware support provided by Policy Feature Card 3 (PFC3), Policy Feature Card 2 (PFC2), Distributed Forwarding Card 3 (DFC3) and Distributed Forwarding Card (DFC):

- Software Features Supported in Hardware by the PFC3, PFC2, DFC3, and DFC, page 1-3
- Software Features Supported in Hardware by the PFC3 and DFC3, page 1-4

Software Features Supported in Hardware by the PFC3, PFC2, DFC3, and DFC

The PFC3, PFC2, DFC3, and DFC 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 MSFC.

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

    ✎
    Note   Idle timeout is processed in software on the MSFC.

  For more information about PFC and DFC support for ACLs, see Chapter 34, "Understanding Cisco IOS ACL Support."

  For complete information about configuring ACLs, refer to 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

- VLAN ACLs (VACLs)—To configure VACLs, see Chapter 35, "Configuring VLAN ACLs."

- 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, refer to 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 MSFC3 address falls within the range of a PBR ACL, traffic addressed to the MSFC3 is policy routed in hardware instead of being forwarded to the MSFC3. To prevent policy routing of traffic addressed to the MSFC3, configure PBR ACLs to deny traffic addressed to the MSFC3.

- Except on MPLS interfaces, TCP intercept—To configure TCP intercept, see the "Configuring TCP Intercept" section on page 33-2.

- Firewall feature set images provide these features:

  - Context-Based Access Control (CBAC) —The PFC installs entries in the NetFlow table to direct flows that require CBAC to the MSFC where the CBAC is applied in software on the MSFC.

  - Authentication Proxy—After authentication on the MSFC, the PFC provides TCAM support for the authentication policy.

  - Port-to-Application Mapping (PAM)—PAM is done in software on the MSFC.

  To configure firewall features, see Chapter 44, "Configuring the Cisco IOS Firewall Feature Set."

- Hardware-assisted NetFlow Aggregation—See "Understanding NDE" section on page 51-2.

Software Features Supported in Hardware by the PFC3 and DFC3

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

- Bidirectional Protocol Independent Multicast (PIM) in hardware—See "Understanding How IPv4 Bidirectional PIM Works" section on page 28-7.

- Multiple-path Unicast Reverse Path Forwarding (RPF) Check—To configure Unicast RPF Check, see the "Configuring Unicast Reverse Path Forwarding Check" section on page 33-2.

- 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 supported only in PFC3BXL or PFC3B 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 MSFC3 to be processed in software. (CSCdz51590)

  To configure NAT, refer to 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 MSFC3, 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)

- With Release 12.2(18)SXE and later releases, IPv4 Multicast over point-to-point generic route encapsulation (GRE) Tunnels—Refer to the publication at this URL:

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

Releases earlier than Release 12.2(18)SXE support IPv4 multicast over point-to-point GRE tunnels in software on the MSFC.

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 MSFC3.

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, refer to 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, refer to this publication:

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. (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.

- The PFC3B and PFC3BXL support PFC QoS features on tunnel interfaces.

- The MSFC3 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, CBAC, and encryption.

Tip For additional information (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/routers/ps368/tsd_products_support_series_home.html