CHAPTER 1

Product Overview

This document provides configuration procedures for the Supervisor Engine 32 and Programmable Intelligent Services Accelerator (PISA). This chapter consists of these sections:

Supported Hardware and Software

For complete information about the chassis, modules, and software features supported by the Supervisor Engine 32 PISA, refer to the *Release Notes for Cisco IOS Release 12.2ZY on the Supervisor Engine 32 PISA*:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/release/notes/ol_13011.html

To configure Network-Based Application Recognition (NBAR) , see this publication:

http://www.cisco.com/en/US/docs/ios/12_4t/qos/configuration/guide/qsnbar1.html

To configure flexible packet matching (FPM), see these publications:

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t4/ht_fpm.html

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/ht_tcdf.html

User Interfaces

Release 12.2ZY 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

The Embedded CiscoView network management system is a web-based interface that uses HTTP and SNMP to provide a graphical representation of the switch 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 switch web page is the enable-level password of the switch.

For more information about web access to the switch, 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 PFC3B

The PFC3B provides 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 PISA.

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

    Note Idle timeout is processed in software on the PISA.

  For more information about PFC3B support for ACLs, see Chapter 31, "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 32, "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 PISA address falls within the range of a PBR ACL, traffic addressed to the PISA is policy routed in hardware instead of being forwarded to the PISA. To prevent policy routing of traffic addressed to the PISA, configure PBR ACLs to deny traffic addressed to the PISA.

- Except on MPLS interfaces, TCP intercept—To configure TCP intercept, see the "Configuring TCP Intercept" section on page 30-2.
- Hardware-assisted NetFlow Aggregation—Refer to this URL:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/nde.html
- Bidirectional Protocol Independent Multicast (PIM) in hardware—See "Understanding How IPv4 Bidirectional PIM Works" section on page 25-6.
- Multiple-path Unicast Reverse Path Forwarding (RPF) Check—To configure Unicast RPF Check, see the "Configuring Unicast Reverse Path Forwarding Check" section on page 30-2.
- Except on MPLS interfaces, Network Address Translation (NAT) for IPv4 unicast and multicast traffic.

  Note the following information about hardware-assisted NAT:

  - The PFC3B does not support NAT of multicast traffic.
  - The PFC3B does not support NAT configured with a route-map that specifies length.
  - When you configure NAT and NDE on an interface, the PFC3B sends all traffic in fragmented packets to the PISA 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 PISA, 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/switches/lan/catalyst6500/ios/12.2ZY/command/reference/M1.html

  (CSCea23296)
- 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

Note The PFC3B does not provide hardware acceleration for tunnels configured with the **tunnel key** command.

- GRE Tunneling and IP in IP Tunneling—The PFC3B supports the following **tunnel** commands:
  - **tunnel destination**
  - **tunnel mode gre**
  - **tunnel mode ipip**
  - **tunnel source**
  - **tunnel ttl**
  - **tunnel tos**

  The PISA supports tunneling configured with any other tunnel commands.

  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/univercd/cc/td/doc/product/software/ios122/122cgcr/finter_r/irfshoip.htm

  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 PFC3B supports PFC QoS features on tunnel interfaces.
  - The PISA 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.