Cisco Persistent Storage Device for Cisco IOS Release 12.2(33)SRD Configuration Guide

October 21, 2008

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco Persistent Storage Device for Cisco IOS Release 12.2(33)SRD Configuration Guide

About Cisco IOS and Cisco IOS XE Software Documentation

Last updated: August 6, 2008

This document describes the objectives, audience, conventions, and organization used in Cisco IOS and Cisco IOS XE software documentation, collectively referred to in this document as Cisco IOS documentation. Also included are resources for obtaining technical assistance, additional documentation, and other information from Cisco. This document is organized into the following sections:

- Documentation Objectives, page i
- Audience, page i
- Documentation Conventions, page ii
- Documentation Organization, page iii
- Additional Resources and Documentation Feedback, page xi

Documentation Objectives

Cisco IOS documentation describes the tasks and commands available to configure and maintain Cisco networking devices.

Audience

The Cisco IOS documentation set is i ntended for users who configure and maintain Cisco networking devices (such as routers and switches) but who may not be familiar with the configuration and maintenance tasks, the relationship among tasks, or the Cisco IOS commands necessary to perform particular tasks. The Cisco IOS documentation set is also intended for those users experienced with Cisco IOS who need to know about new features, new configuration options, and new software characteristics in the current Cisco IOS release.

Documentation Conventions

In Cisco IOS documentation, the term *router* may be used to refer to various Cisco products; for example, routers, access servers, and switches. These and other networking devices that support Cisco IOS software are shown interchangeably in examples and are used only for illustrative purposes. An example that shows one product does not necessarily mean that other products are not supported.

This section includes the following topics:

- Typographic Conventions, page ii
- Command Syntax Conventions, page ii
- Software Conventions, page iii
- Reader Alert Conventions, page iii

Typographic Conventions

Cisco IOS documentation uses the following typographic conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
string	A string is a nonquoted set of characters shown in italics. For example, when setting a Simple Network Management Protocol (SNMP) community string to *public*, do not use quotation marks around the string; otherwise, the string will include the quotation marks.

Command Syntax Conventions

Cisco IOS documentation uses the following command syntax conventions:

Convention	Description
bold	Bold text indicates commands and keywords that you enter as shown.
italic	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional keyword or argument.
|	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x | y]	Square brackets enclosing keywords or arguments separated by a pipe indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a pipe indicate a required choice.
[x {y | z}]	Braces and a pipe within square brackets indicate a required choice within an optional element.

Software Conventions

Cisco IOS uses the following program code conventions:

Convention	Description
`Courier font`	Courier font is used for information that is displayed on a PC or terminal screen.
`Bold Courier font`	Bold Courier font indicates text that the user must enter.
< >	Angle brackets enclose text that is not displayed, such as a password. Angle brackets also are used in contexts in which the italic font style is not supported; for example, ASCII text.
!	An exclamation point at the beginning of a line indicates that the text that follows is a comment, not a line of code. An exclamation point is also displayed by Cisco IOS software for certain processes.
[ ]	Square brackets enclose default responses to system prompts.

Reader Alert Conventions

The Cisco IOS documentation set uses the following conventions for reader alerts:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Documentation Organization

This section describes the Cisco IOS documentation set, how it is organized, and how to access it on Cisco.com. Included are lists of configuration guides, command references, and supplementary references and resources that make up the documentation set. The following topics are included:

- Cisco IOS Documentation Set, page iv
- Cisco IOS Documentation on Cisco.com, page iv
- Configuration Guides, Command References, and Supplementary Resources, page v

Cisco IOS Documentation Set

Cisco IOS documentation consists of the following:

- Release notes and caveats provide information about platform, technology, and feature support for a release and describe severity 1 (catastrophic), severity 2 (severe), and severity 3 (moderate) defects in released Cisco IOS code. Review release notes before other documents to learn whether or not updates have been made to a feature.
- Sets of configuration guides and command references organized by technology and published for each standard Cisco IOS release.
  - Configuration guides—Compilations of documents that provide informational and task-oriented descriptions of Cisco IOS features.
  - Command references—Compilations of command pages that provide detailed information about the commands used in the Cisco IOS features and processes that make up the related configuration guides. For each technology, there is a single command reference that covers all Cisco IOS releases and that is updated at each standard release.
- Lists of all the commands in a specific release and all commands that are new, modified, removed, or replaced in the release.
- Command reference book for **debug** commands. Command pages are listed in alphabetical order.
- Reference book for system messages for all Cisco IOS releases.

Cisco IOS Documentation on Cisco.com

The following sections describe the documentation organization and how to access various document types.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

New Features List

The New Features List for each release provides a list of all features in the release with hyperlinks to the feature guides in which they are documented.

Feature Guides

Cisco IOS features are documented in feature guides. Feature guides describe one feature or a group of related features that are supported on many different software releases and platforms. Your Cisco IOS software release or platform may not support all the features documented in a feature guide. See the Feature Information table at the end of the feature guide for information about which features in that guide are supported in your software release.

Configuration Guides

Configuration guides are provided by technology and release and comprise a set of individual feature guides relevant to the release and technology.

Command References

Command reference books describe Cisco IOS commands that are supported in many different software releases and on many different platforms. The books are provided by technology. For information about all Cisco IOS commands, use the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or the *Cisco IOS Master Command List, All Releases*, at http://www.cisco.com/en/US/docs/ios/mcl/all_release/all_mcl.html.

Cisco IOS Supplementary Documents and Resources

Supplementary documents and resources are listed in Table 2 on page xi.

Configuration Guides, Command References, and Supplementary Resources

Table 1 lists, in alphabetical order, Cisco IOS and Cisco IOS XE software configuration guides and command references, including brief descriptions of the contents of the documents. The Cisco IOS command references are comprehensive, meaning that they include commands for both Cisco IOS software and Cisco IOS XE software, for all releases. The configuration guides and command references support many different software releases and platforms. Your Cisco IOS software release or platform may not support all these technologies.

For additional information about configuring and operating specific networking devices, go to the Product Support area of Cisco.com at http://www.cisco.com/web/psa/products/index.html.

Table 2 lists documents and resources that supplement the Cisco IOS software configuration guides and command references. These supplementary resources include release notes and caveats; master command lists; new, modified, removed, and replaced command lists; system messages; and the debug command reference.

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS AppleTalk Configuration Guide *Cisco IOS XE AppleTalk Configuration Guide* *Cisco IOS AppleTalk Command Reference*	AppleTalk protocol.
Cisco IOS Asynchronous Transfer Mode Configuration Guide *Cisco IOS Asynchronous Transfer Mode Command Reference*	LAN ATM, multiprotocol over ATM (MPoA), and WAN ATM.

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS Bridging and IBM Networking Configuration Guide *Cisco IOS Bridging Command Reference* *Cisco IOS IBM Networking Command Reference*	• Transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and token ring route switch module (TRRSM). • Data-link switching plus (DLSw+), serial tunnel (STUN), block serial tunnel (BSTUN); logical link control, type 2 (LLC2), synchronous data link control (SDLC); IBM Network Media Translation, including Synchronous Data Logical Link Control (SDLLC) and qualified LLC (QLLC); downstream physical unit (DSPU), Systems Network Architecture (SNA) service point, SNA frame relay access, advanced peer-to-peer networking (APPN), native client interface architecture (NCIA) client/server topologies, and IBM Channel Attach.
Cisco IOS Broadband and DSL Configuration Guide *Cisco IOS XE Broadband and DSL Configuration Guide* *Cisco IOS Broadband and DSL Command Reference*	Point-to-Point Protocol (PPP) over ATM (PPPoA) and PPP over Ethernet (PPPoE).
Cisco IOS Carrier Ethernet Configuration Guide *Cisco IOS Carrier Ethernet Command Reference*	Connectivity fault management (CFM), Ethernet Local Management Interface (ELMI), IEEE 802.3ad link bundling, Link Layer Discovery Protocol (LLDP), media endpoint discovery (MED), and operations, administration, and maintenance (OAM).
Cisco IOS Configuration Fundamentals Configuration Guide *Cisco IOS XE Configuration Fundamentals Configuration Guide* *Cisco IOS Configuration Fundamentals Command Reference*	Autoinstall, Setup, Cisco IOS command-line interface (CLI), Cisco IOS file system (IFS), Cisco IOS web browser user interface (UI), basic file transfer services, and file management.
Cisco IOS DECnet Configuration Guide *Cisco IOS XE DECnet Configuration Guide* *Cisco IOS DECnet Command Reference*	DECnet protocol.
Cisco IOS Dial Technologies Configuration Guide *Cisco IOS XE Dial Technologies Configuration Guide* *Cisco IOS Dial Technologies Command Reference*	Asynchronous communications, dial backup, dialer technology, dial-in terminal services and AppleTalk remote access (ARA), large scale dialout, dial-on-demand routing, dialout, modem and resource pooling, ISDN, multilink PPP (MLP), PPP, virtual private dialup network (VPDN).
Cisco IOS Flexible NetFlow Configuration Guide *Cisco IOS Flexible NetFlow Command Reference*	Flexible NetFlow.

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS H.323 Configuration Guide	Gatekeeper enhancements for managed voice services, Gatekeeper Transaction Message Protocol, gateway codec order preservation and shutdown control, H.323 dual tone multifrequency relay, H.323 version 2 enhancements, Network Address Translation (NAT) support of H.323 v2 Registration, Admission, and Status (RAS) protocol, tokenless call authorization, and VoIP gateway trunk and carrier-based routing.
Cisco IOS High Availability Configuration Guide *Cisco IOS XE High Availability Configuration Guide* *Cisco IOS High Availability Command Reference*	A variety of High Availability (HA) features and technologies that are available for different network segments (from enterprise access to service provider core) to facilitate creation of end-to-end highly available networks. Cisco IOS HA features and technologies can be categorized in three key areas: system-level resiliency, network-level resiliency, and embedded management for resiliency.
Cisco IOS Integrated Session Border Controller Command Reference	A VoIP-enabled device that is deployed at the edge of networks. An SBC is a toolkit of functions, such as signaling interworking, network hiding, security, and quality of service (QoS).
Cisco IOS Intelligent Service Gateway Configuration Guide *Cisco IOS Intelligent Service Gateway Command Reference*	Subscriber identification, service and policy determination, session creation, session policy enforcement, session life-cycle management, accounting for access and service usage, session state monitoring.
Cisco IOS Interface and Hardware Component Configuration Guide *Cisco IOS XE Interface and Hardware Component Configuration Guide* *Cisco IOS Interface and Hardware Component Command Reference*	LAN interfaces, logical interfaces, serial interfaces, virtual interfaces, and interface configuration.
Cisco IOS IP Addressing Services Configuration Guide *Cisco IOS XE Addressing Services Configuration Guide* *Cisco IOS IP Addressing Services Command Reference*	Address Resolution Protocol (ARP), Network Address Translation (NAT), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Next Hop Address Resolution Protocol (NHRP).
Cisco IOS IP Application Services Configuration Guide *Cisco IOS XE IP Application Services Configuration Guide* *Cisco IOS IP Application Services Command Reference*	Enhanced Object Tracking (EOT), Gateway Load Balancing Protocol (GLBP), Hot Standby Router Protocol (HSRP), IP Services, Server Load Balancing (SLB), Stream Control Transmission Protocol (SCTP), TCP, Web Cache Communication Protocol (WCCP), User Datagram Protocol (UDP), and Virtual Router Redundancy Protocol (VRRP).
Cisco IOS IP Mobility Configuration Guide *Cisco IOS IP Mobility Command Reference*	Mobile ad hoc networks (MANet) and Cisco mobile networks.
Cisco IOS IP Multicast Configuration Guide *Cisco IOS XE IP Multicast Configuration Guide* *Cisco IOS IP Multicast Command Reference*	Protocol Independent Multicast (PIM) sparse mode (PIM-SM), bidirectional PIM (bidir-PIM), Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), Internet Group Management Protocol (IGMP), and Multicast VPN (MVPN).

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS IP Routing Protocols Configuration Guide *Cisco IOS XE IP Routing Protocols Configuration Guide* *Cisco IOS IP Routing Protocols Command Reference*	Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast, bidirectional forwarding detection (BFD), Enhanced Interior Gateway Routing Protocol (EIGRP), Interior Gateway Routing Protocol (IGRP), Intermediate System-to-Intermediate System (IS-IS), on-demand routing (ODR), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).
Cisco IOS IP SLAs Configuration Guide *Cisco IOS XE IP SLAs Configuration Guide* *Cisco IOS IP SLAs Command Reference*	Cisco IOS IP Service Level Agreements (IP SLAs).
Cisco IOS IP Switching Configuration Guide *Cisco IOS XE IP Switching Configuration Guide* *Cisco IOS IP Switching Command Reference*	Cisco Express Forwarding, fast switching, and Multicast Distributed Switching (MDS).
Cisco IOS IPv6 Configuration Guide *Cisco IOS XE IPv6 Configuration Guide* *Cisco IOS IPv6 Command Reference*	For IPv6 features, protocols, and technologies, go to the IPv6 “Start Here” document at the following URL: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html
Cisco IOS ISO CLNS Configuration Guide *Cisco IOS XE ISO CLNS Configuration Guide* *Cisco IOS ISO CLNS Command Reference*	ISO connectionless network service (CLNS).
Cisco IOS LAN Switching Configuration Guide *Cisco IOS XE LAN Switching Configuration Guide* *Cisco IOS LAN Switching Command Reference*	VLANs, Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, IEEE 802.1Q encapsulation, and multilayer switching (MLS).
Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide *Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference*	Cisco IOS Gateway GPRS Support Node (GGSN) in a 2.5-generation general packet radio service (GPRS) and 3-generation universal mobile telecommunication system (UMTS) network.
Cisco IOS Mobile Wireless Home Agent Configuration Guide *Cisco IOS Mobile Wireless Home Agent Command Reference*	Cisco Mobile Wireless Home Agent, an anchor point for mobile terminals for which mobile IP or proxy mobile IP services are provided.
Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide *Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference*	Cisco Packet Data Serving Node (PDSN), a wireless gateway that is between the mobile infrastructure and standard IP networks and that enables packet data services in a code division multiple access (CDMA) environment.
Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide *Cisco IOS Mobile Wireless Radio Access Networking Command Reference*	Cisco IOS radio access network products.

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS Multiprotocol Label Switching Configuration Guide *Cisco IOS XE Multiprotocol Label Switching Configuration Guide* *Cisco IOS Multiprotocol Label Switching Command Reference*	MPLS Label Distribution Protocol (LDP), MPLS Layer 2 VPNs, MPLS Layer 3 VPNs, MPLS Traffic Engineering (TE), and MPLS Embedded Management (EM) and MIBs.
Cisco IOS Multi-Topology Routing Configuration Guide *Cisco IOS Multi-Topology Routing Command Reference*	Unicast and multicast topology configurations, traffic classification, routing protocol support, and network management support.
Cisco IOS NetFlow Configuration Guide *Cisco IOS XE NetFlow Configuration Guide* *Cisco IOS NetFlow Command Reference*	Network traffic data analysis, aggregation caches, export features.
Cisco IOS Network Management Configuration Guide *Cisco IOS XE Network Management Configuration Guide* *Cisco IOS Network Management Command Reference*	Basic system management; system monitoring and logging; troubleshooting, logging, and fault management; Cisco Discovery Protocol; Cisco IOS Scripting with Tool Control Language (Tcl); Cisco networking services (CNS); DistributedDirector; Embedded Event Manager (EEM); Embedded Resource Manager (ERM); Embedded Syslog Manager (ESM); HTTP; Remote Monitoring (RMON); SNMP; and VPN Device Manager Client for Cisco IOS Software (XSM Configuration).
Cisco IOS Novell IPX Configuration Guide *Cisco IOS XE Novell IPX Configuration Guide* *Cisco IOS Novell IPX Command Reference*	Novell Internetwork Packet Exchange (IPX) protocol.
Cisco IOS Optimized Edge Routing Configuration Guide *Cisco IOS Optimized Edge Routing Command Reference*	Optimized edge routing (OER) monitoring, policy configuration, routing control, logging and reporting, and VPN IPsec/generic routing encapsulation (GRE) tunnel interface optimization.
Cisco IOS Quality of Service Solutions Configuration Guide *Cisco IOS XE Quality of Service Solutions Configuration Guide* *Cisco IOS Quality of Service Solutions Command Reference*	Class-based weighted fair queuing (CBWFQ), custom queuing, distributed traffic shaping (DTS), generic traffic shaping (GTS), IP- to-ATM class of service (CoS), low latency queuing (LLQ), modular QoS CLI (MQC), Network-Based Application Recognition (NBAR), priority queuing, Security Device Manager (SDM), Multilink PPP (MLPPP) for QoS, header compression, AutoQoS, QoS features for voice, Resource Reservation Protocol (RSVP), weighted fair queuing (WFQ), and weighted random early detection (WRED).
Cisco IOS Security Configuration Guide *Cisco IOS XE Security Configuration Guide* *Cisco IOS Security Command Reference*	Access control lists (ACLs), authentication, authorization, and accounting (AAA), firewalls, IP security and encryption, neighbor router authentication, network access security, network data encryption with router authentication, public key infrastructure (PKI), RADIUS, TACACS+, terminal access security, and traffic filters.

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS Service Selection Gateway Configuration Guide *Cisco IOS Service Selection Gateway Command Reference*	Subscriber authentication, service access, and accounting.
Cisco IOS Software Activation Configuration Guide *Cisco IOS Software Activation Command Reference*	An orchestrated collection of processes and components to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses.
Cisco IOS Software Modularity Installation and Configuration Guide *Cisco IOS Software Modularity Command Reference*	Installation and basic configuration of software modularity images, including installations on single and dual route processors, installation rollbacks, software modularity binding, software modularity processes and patches.
Cisco IOS Terminal Services Configuration Guide *Cisco IOS Terminal Services Command Reference* *Cisco IOS XE Terminal Services Command Reference*	DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD).
Cisco IOS Virtual Switch Command Reference	Virtual switch redundancy, high availability, and packet handling; converting between standalone and virtual switch modes; virtual switch link (VSL); Virtual Switch Link Protocol (VSLP). **Note** For information about virtual switch configuration, refer to the product-specific software configuration information for the Cisco Catalyst 6500 series switch or for the Metro Ethernet 6500 series switch.
Cisco IOS Voice Configuration Library *Cisco IOS Voice Command Reference*	Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. The library includes documentation for IP telephony applications.
Cisco IOS VPDN Configuration Guide *Cisco IOS XE VPDN Configuration Guide* *Cisco IOS VPDN Command Reference*	Layer 2 Tunneling Protocol (L2TP) dial-out load balancing and redundancy, L2TP extended failover, L2TP security VPDN, multihop by Dialed Number Identification Service (DNIS), timer and retry enhancements for L2TP and Layer 2 Forwarding (L2F), RADIUS Attribute 82: tunnel assignment ID, shell-based authentication of VPDN users, tunnel authentication via RADIUS on tunnel terminator.
Cisco IOS Wide-Area Networking Configuration Guide *Cisco IOS XE Wide-Area Networking Configuration Guide* *Cisco IOS Wide-Area Networking Command Reference*	Frame Relay, Layer 2 Tunneling Protocol Version 3 (L2TPv3), Link Access Procedure, Balanced (LAPB), Switched Multimegabit Data Service (SMDS), and X.25.
Cisco IOS Wireless LAN Configuration Guide *Cisco IOS Wireless LAN Command Reference*	Broadcast key rotation, IEEE 802.11x support, IEEE 802.1x authenticator, IEEE 802.1x local authentication service for Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Multiple Basic Service Set ID (BSSID), Wi-Fi Multimedia (WMM) required elements, and Wi-Fi Protected Access (WPA).

Table 2 Cisco IOS Supplementary Documents and Resources

Document Title	Description
Cisco IOS Master Command List, All Releases	Alphabetical list of all the commands documented in all Cisco IOS releases.
Cisco IOS New, Modified, Removed, and Replaced Commands	List of all the new, modified, removed, and replaced commands for a Cisco IOS release.
Cisco IOS Software System Messages	List of Cisco IOS system messages and descriptions. System messages may indicate problems with your system; be informational only; or may help diagnose problems with communications lines, internal hardware, or the system software.
Cisco IOS Debug Command Reference	Alphabetical list of **debug** commands including brief descriptions of use, command syntax, and usage guidelines.
Release Notes and Caveats	Information about new and changed features, system requirements, and other useful information about specific software releases; information about defects in specific Cisco IOS software releases.
MIBs	Files used for network monitoring. To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator at the following URL: http://www.cisco.com/go/mibs
RFCs	Standards documents maintained by the Internet Engineering Task Force (IETF) that Cisco IOS documentation references where applicable. The full text of referenced RFCs may be obtained at the following URL: http://www.rfc-editor.org/

Additional Resources and Documentation Feedback

What's New in Cisco Product Documentation is published monthly and describes all new and revised Cisco technical documentation. The *What's New in Cisco Product Documentation* publication also provides information about obtaining the following resources:

- Technical documentation
- Cisco product security overview
- Product alerts and field notices
- Technical assistance

Cisco IOS technical documentation includes embedded feedback forms where you can rate documents and provide suggestions for improvement. Your feedback helps us improve our documentation.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Using the Command-Line Interface in Cisco IOS and Cisco IOS XE Software

Last updated: August 6, 2008

This document provides basic information about the command-line interface (CLI) in Cisco IOS and Cisco IOS XE software and how you can use some of the CLI features. This document contains the following sections:

For more information about using the CLI, see the "Using the Cisco IOS Command-Line Interface" section of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

For information about the software documentation set, see the "About Cisco IOS and Cisco IOS XE Software Documentation" document.

Initially Configuring a Device

Initially configuring a device varies by platform. For information about performing an initial configuration, see the hardware installation documentation that is provided with the original packaging of the product or go to the Product Support area of Cisco.com at http://www.cisco.com/web/psa/products/index.html.

After you have performed the initial configuration and connected the device to your network, you can configure the device by using the console port or a remote access method, such as Telnet or Secure Shell (SSH), to access the CLI or by using the configuration method provided on the device, such as Security Device Manager.

Changing the Default Settings for a Console or AUX Port

There are only two changes that you can make to a console port and an AUX port:

- Change the port speed with the **config-register 0x** command. Changing the port speed is not recommended. The well-known default speed is 9600.
- Change the behavior of the port; for example, by adding a password or changing the timeout value.

Note The AUX port on the Route Processor (RP) installed in a Cisco ASR1000 series router does not serve any useful customer purpose and should be accessed only under the advisement of a customer support representative.

Using the CLI

This section describes the following topics:

- Understanding Command Modes, page ii
- Using the Interactive Help Feature, page v
- Understanding Command Syntax, page vi
- Understanding Enable and Enable Secret Passwords, page viii
- Using the Command History Feature, page viii
- Abbreviating Commands, page ix
- Using Aliases for CLI Commands, page ix
- Using the no and default Forms of Commands, page x
- Using the debug Command, page x
- Filtering Output Using Output Modifiers, page x
- Understanding CLI Error Messages, page xi

Understanding Command Modes

The CLI command mode structure is hierarchical, and each mode supports a set of specific commands. This section describes the most common of the many modes that exist.

Table 1 lists common command modes with associated CLI prompts, access and exit methods, and a brief description of how each mode is used.

Table 1 CLI Command Modes

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
User EXEC	Log in.	`Router>`	Issue the **logout** or **exit** command.	• Change terminal settings. • Perform basic tests. • Display device status.
Privileged EXEC	From user EXEC mode, issue the **enable** command.	`Router#`	Issue the **disable** command or the **exit** command to return to user EXEC mode.	• Issue **show** and **debug** commands. • Copy images to the device. • Reload the device. • Manage device configuration files. • Manage device file systems.
Global configuration	From privileged EXEC mode, issue the **configure terminal** command.	`Router(config)#`	Issue the **exit** command or the **end** command to return to privileged EXEC mode.	Configure the device.
Interface configuration	From global configuration mode, issue the **interface** command.	`Router(config-if)#`	Issue the **exit** command to return to global configuration mode or the **end** command to return to privileged EXEC mode.	Configure individual interfaces.
Line configuration	From global configuration mode, issue the **line vty** or **line console** command.	`Router(config-line)#`	Issue the **exit** command to return to global configuration mode or the **end** command to return to privileged EXEC mode.	Configure individual terminal lines.

Table 1 CLI Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
ROM monitor	From privileged EXEC mode, issue the **reload** command. Press the **Break** key during the first 60 seconds while the system is booting.	`rommon # >` The # symbol represents the line number and increments at each prompt.	Issue the **continue** command.	• Run as the default operating mode when a valid image cannot be loaded. • Access the fall-back procedure for loading an image when the device lacks a valid image and cannot be booted. • Perform password recovery when a CTRL-Break sequence is issued within 60 seconds of a power-on or reload event.
Diagnostic (available only on the Cisco ASR1000 series router)	The router boots or enters diagnostic mode in the following scenarios. When a Cisco IOS process or processes fail, in most scenarios the router will reload. • A user-configured access policy was configured using the **transport-map** command, which directed the user into diagnostic mode. • The router was accessed using an RP auxiliary port. • A break signal (**Ctrl-C**, **Ctrl-Shift-6**, or the **send break** command) was entered, and the router was configured to enter diagnostic mode when the break signal was received.	`Router(diag)#`	If a Cisco IOS process failure is the reason for entering diagnostic mode, the failure must be resolved and the router must be rebooted to exit diagnostic mode. If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or using a method that is configured to connect to the Cisco IOS CLI. If the RP auxiliary port was used to access the router, use another port for access. Accessing the router through the auxiliary port is not useful for customer purposes.	• Inspect various states on the router, including the Cisco IOS state. • Replace or roll back the configuration. • Provide methods of restarting the Cisco IOS software or other processes. • Reboot hardware, such as the entire router, an RP, an ESP, a SIP, a SPA, or possibly other hardware components. • Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.

EXEC commands are not saved when the software reboots. Commands that you issue in a configuration mode can be saved to the startup configuration. If you save the running configuration to the startup configuration, these commands will execute when the software is rebooted. Global configuration mode is the highest level of configuration mode. From global configuration mode, you can enter a variety of other configuration modes, including protocol-specific modes.

ROM monitor mode is a separate mode that is used when the software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode. Use the question symbol (?) to view the commands that you can use while the device is in ROM monitor mode.

```
rommon 1 > ?
alias                set and display aliases command
boot                 boot up an external process
confreg              configuration register utility
cont                 continue executing a downloaded image
context              display the context of a loaded image
cookie               display contents of cookie PROM in hex
.
.
.
rommon 2 >
```

The following example shows how the command prompt changes to indicate a different command mode:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 1/1
Router(config-if)# ethernet
Router(config-line)# exit
Router(config)# end
Router#
```

Note A keyboard alternative to the **end** command is Ctrl-Z.

Using the Interactive Help Feature

The CLI includes an interactive Help feature. Table 2 describes how to use the Help feature.

Table 2 CLI Interactive Help Commands

Command	Purpose
help	Provides a brief description of the help feature in any command mode.
?	Lists all commands available for a particular command mode.
*partial command***?**	Provides a list of commands that begin with the character string (no space between the command and the question mark).
partial command<**Tab**>	Completes a partial command name (no space between the command and <Tab>).
command **?**	Lists the keywords, arguments, or both associated with the command (space between the command and the question mark).
command keyword **?**	Lists the arguments that are associated with the keyword (space between the keyword and the question mark).

The following examples show how to use the help commands:

help

```
Router> help

Help may be requested at any point in a command by entering a question mark '?'.  If
nothing matches, the help list will be empty and you must backup until entering a '?'
shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?')
and describes each possible argument.

2. Partial help is provided when an abbreviated argument is entered and you want to know
what arguments match the input (e.g. 'show pr?'.)
```

?

```
Router# ?
Exec commands:
  access-enable        Create a temporary access-List entry
  access-profile       Apply user-profile to interface
  access-template      Create a temporary access-List entry
  alps                 ALPS exec commands
  archive              manage archive files
<snip>
```

partial command?

```
Router(config)# zo?
zone  zone-pair
```

partial command<Tab>

```
Router(config)# we<Tab> webvpn
```

command ?

```
Router(config-if)# pppoe ?
  enable        Enable pppoe
  max-sessions  Maximum PPPOE sessions
```

command keyword ?

```
Router(config-if)# pppoe enable ?
  group  attach a BBA group
  <cr>
```

Understanding Command Syntax

Command syntax is the format in which a command should be entered in the CLI. Commands include the name of the command, keywords, and arguments. Keywords are alphanumeric strings that are used literally. Arguments are placeholders for values that a user must supply. Keywords and arguments may be required or optional.

Specific conventions convey information about syntax and command elements. Table 3 describes these conventions.

Table 3 CLI Syntax Conventions

Symbol/Text	Function	Notes
< > (angle brackets)	Indicate that the option is an argument.	Sometimes arguments are displayed without angle brackets.
A.B.C.D.	Indicates that you must enter a dotted decimal IP address.	Angle brackets (< >) are not always used to indicate that an IP address is an argument.
WORD (all capital letters)	Indicates that you must enter one word.	Angle brackets (< >) are not always used to indicate that a WORD is an argument.
LINE (all capital letters)	Indicates that you must enter more than one word.	Angle brackets (< >) are not always used to indicate that a LINE is an argument.
<cr> (carriage return)	Indicates the end of the list of available keywords and arguments, and also indicates when keywords and arguments are optional. When <cr> is the only option, you have reached the end of the branch or the end of the command if the command has only one branch.	—

The following examples show syntax conventions:

```
Router(config)# ethernet cfm domain ?
  WORD  domain name
Router(config)# ethernet cfm domain dname ?
  level
Router(config)# ethernet cfm domain dname level ?
  <0-7>  maintenance level number
Router(config)# ethernet cfm domain dname level 7 ?
  <cr>
Router(config)# snmp-server file-transfer access-group 10 ?
  protocol  protocol options
  <cr>
Router(config)# logging host ?
  Hostname or A.B.C.D  IP address of the syslog server
  ipv6                 Configure IPv6 syslog server
Router(config)# snmp-server file-transfer access-group 10 ?
  protocol  protocol options
  <cr>
```

Understanding Enable and Enable Secret Passwords

Some privileged EXEC commands are used for actions that impact the system, and it is recommended that you set a password for these commands to prevent unauthorized use. Two types of passwords, enable (not encrypted) and enable secret (encrypted), can be set. The following commands set these passwords and are issued in global configuration mode:

- **enable** *password*
- **enable secret** *password*

Using an enable secret password is recommended because it is encrypted and more secure than the enable password. When you use an enable secret password, text is encrypted (unreadable) before it is written to the config.text file. When you use an enable password, the text is written as entered (readable) to the config.text file.

Each type of password is case sensitive, can contain from 1 to 25 uppercase and lowercase alphanumeric characters, and can start with a number. Spaces are also valid password characters; for example, “two words” is a valid password. Leading spaces are ignored, but trailing spaces are recognized.

Note Both password commands have numeric keywords that are single integer values. If you choose a number for the first character of your password followed by a space, the system will read the number as if it were the numeric keyword and not as part of your password.

When both passwords are set, the enable secret password takes precedence over the enable password.

To remove a password, use the **no** form of the commands: **no enable** *password* or **no enable secret** *password*.

For more information about password recovery procedures for Cisco products, see http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml.

Using the Command History Feature

The CLI command history feature saves the commands you enter during a session in a command history buffer. The default number of commands saved is 10, but the number is configurable within the range of 0 to 256. This command history feature is particularly useful for recalling long or complex commands.

To change the number of commands saved in the history buffer for a terminal session, issue the **terminal history size** command:

```
Router# terminal history size num
```

A command history buffer is also available in line configuration mode with the same default and configuration options. To set the command history buffer size for a terminal session in line configuration mode, issue the **history** command:

```
Router(config-line)# history [size num]
```

To recall commands from the history buffer, use the following methods:

- Press Ctrl-P or the up arrow key—Recalls commands beginning with the most recent command. Repeat the key sequence to recall successively older commands.

- Press Ctrl-N or the down arrow key—Recalls the most recent commands in the history buffer after they have been recalled using Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.

Note The arrow keys function only on ANSI-compatible terminals such as the VT100.

- Issue the **show history** command in user EXEC or privileged EXEC mode—Lists the most recent commands that you entered. The number of commands that are displayed is determined by the setting of the **terminal history size** and **history** commands.

  The CLI command history feature is enabled by default. To disable this feature for a terminal session, issue the **terminal no history** command in user EXEC or privileged EXEC mode or the **no history** command in line configuration mode.

Abbreviating Commands

Typing a complete command name is not always required for the command to execute. The CLI recognizes an abbreviated command when the abbreviation contains enough characters to uniquely identify the command. For example, the **show version** command can be abbreviated as **sh ver**. It cannot be abbreviated as **s ver** because **s** could mean **show**, **set**, or **systat**. The **sh v** abbreviation also is not valid because the **show** command has **vrrp** as a keyword in addition to **version**. (Command and keyword examples from Cisco IOS Release 12.4(13)T.)

Using Aliases for CLI Commands

To save time and the repetition of entering the same command multiple times, you can use a command alias. An alias can be configured to do anything that can be done at the command line, but an alias cannot move between modes, type in passwords, or perform any interactive functions.

Table 4 shows the default command aliases.

Table 4 Default Command Aliases

Command Alias	Original Command
h	help
lo	logout
p	ping
s	show
u or **un**	undebug
w	where

To create a command alias, issue the **alias** command in global configuration mode. The syntax of the command is **alias** *mode command-alias original-command*. Following are some examples:

- Router(config)# **alias exec prt partition**—privileged EXEC mode
- Router(config)# **alias configure sb source-bridge**—global configuration mode
- Router(config)# **alias interface rl rate-limit**—interface configuration mode

To view both default and user-created aliases, issue the **show alias** command.

For more information about the **alias** command, see
http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html.

Using the no and default Forms of Commands

Most configuration commands have a **no** form that is used to reset a command to its default value or disable a feature or function. For example, the **ip routing** command is enabled by default. To disable this command, you would issue the **no ip routing** command. To re-enable IP routing, you would issue the **ip routing** command.

Configuration commands may also have a **default** form, which returns the command settings to their default values. For commands that are disabled by default, using the **default** form has the same effect as using the **no** form of the command. For commands that are enabled by default and have default settings, the **default** form enables the command and returns the settings to their default values.

The **no** and **default** forms of commands are described in the command pages of command references.

Using the debug Command

A **debug** command produces extensive output that helps you troubleshoot problems in your network. These commands are available for many features and functions within Cisco IOS and Cisco IOS XE software. Some **debug** commands are **debug all**, **debug aaa accounting**, and **debug mpls packets**. To use **debug** commands during a Telnet session with a device, you must first enter the **terminal monitor** command. To turn off debugging completely, you must enter the **undebug all** command.

For more information about **debug** commands, see the *Cisco IOS Debug Command Reference* at http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html.

⚠ **Caution** Debugging is a high priority and high CPU utilization process that can render your device unusable. Use **debug** commands only to troubleshoot specific problems. The best times to run debugging are during periods of low network traffic and when few users are interacting with the network. Debugging during these periods decreases the likelihood that the **debug** command processing overhead will affect network performance or user access or response times.

Filtering Output Using Output Modifiers

Many commands produce lengthy output that may use several screens to display. Using output modifiers, you can filter this output to show only the information that you want to see.

Three output modifiers are available and are described as follows:

- **begin** *regular expression*—Displays the first line in which a match of the regular expression is found and all lines that follow.
- **include** *regular expression*—Displays all lines in which a match of the regular expression is found.
- **exclude** *regular expression*—Displays all lines except those in which a match of the regular expression is found.

To use one of these output modifiers, type the command followed by the pipe symbol (|), the modifier, and the regular expression that you want to search for or filter. A regular expression is a case-sensitive alphanumeric pattern. It can be a single character or number, a phrase, or a more complex string.

The following example illustrates how to filter output of the **show interface** command to display only lines that include the expression "protocol."

```
Router# show interface | include protocol

FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

Understanding CLI Error Messages

You may encounter some error messages while using the CLI. Table 5 shows the common CLI error messages.

Table 5 Common CLI Error Messages

Error Message	Meaning	How to Get Help
% Ambiguous command: "show con"	You did not enter enough characters for the command to be recognized.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Incomplete command.	You did not enter all the keywords or values required by the command.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Invalid input detected at "^" marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all the commands that are available in this command mode. The keywords that you are allowed to enter for the command appear.

For more system error messages, see the following documents:

- *Cisco IOS Release 12.2SR System Message Guide*
- *Cisco IOS System Messages, Volume 1 of 2* (Cisco IOS Release 12.4)
- *Cisco IOS System Messages, Volume 2 of 2* (Cisco IOS Release 12.4)

Saving Changes to a Configuration

To save changes that you made to the configuration of a device, you must issue the **copy running-config startup-config** command or the **copy system:running-config nvram:startup-config** command. When you issue these commands, the configuration changes that you made are saved to the startup configuration and saved when the software reloads or power to the device is turned off or interrupted. The following example shows the syntax of the **copy running-config startup-config** command:

```
Router# copy running-config startup-config
Destination filename [startup-config]?
```

You press Enter to accept the startup-config filename (the default), or type a new filename and then press Enter to accept that name. The following output is displayed indicating that the configuration was saved:

```
Building configuration...
[OK]
Router#
```

On most platforms, the configuration is saved to NVRAM. On platforms with a Class A flash file system, the configuration is saved to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM.

Additional Information

- "Using the Cisco IOS Command-Line Interface" section of the *Cisco IOS Configuration Fundamentals Configuration Guide*:

  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html

  or

  "Using Cisco IOS XE Software" chapter of the *Cisco ASR1000 Series Aggregation Services Routers Software Configuration Guide*:

  http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/using_cli.html

- Cisco Product Support Resources

  http://www.cisco.com/web/psa/products/index.html

- Support area on Cisco.com (also search for documentation by task or product)

  http://www.cisco.com/en/US/support/index.html

- *White Paper: Cisco IOS Reference Guide*

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_white_paper09186a008018305e.shtml

- Software Download Center (downloads; tools; licensing, registration, advisory, and general information) (requires Cisco.com User ID and password)

  http://www.cisco.com/kobayashi/sw-center/

- Error Message Decoder, a tool to help you research and resolve error messages for Cisco IOS software

  http://www.cisco.com/pcgi-bin/Support/Errordecoder/index.cgi

- Command Lookup Tool, a tool to help you find detailed descriptions of Cisco IOS commands (requires Cisco.com user ID and password)

  http://tools.cisco.com/Support/CLILookup

- Output Interpreter, a troubleshooting tool that analyzes command output of supported **show** commands

  https://www.cisco.com/pcgi-bin/Support/OutputInterpreter/home.pl\

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

CHAPTER 1

Cisco Persistent Storage Device Module Installation and Configuration Guide

WS-SVC-PSD-1

This publication describes how to install and configure the Cisco Persistent Storage Device (PSD) on the Catalyst 6500 series switch. See the "Related Documentation" section on page 1-51 for more information about software configuration for the switch.

Note For translations of the warnings in this publication, see the "Safety Overview" section on page 1-8 and refer to the *Regulatory Compliance and Safety Information* for the Catalyst 6500 series switches.

Contents

This publication consists of these sections:

Overview

This section describes the Catalyst 6500 and 7600 series PSD, how it operates, and how to manage it, and includes these sections:

- Understanding How the PSD Works, page 1-2
- Configuring and Managing the PSD, page 1-4
- Front Panel Description, page 1-6
- Specifications, page 1-7

Understanding How the PSD Works

The Cisco Persistent Storage Device (PSD) provides persistent storage capabilities to Cisco clients, and allows the clients to store data on the PSD's internal hard drive. Release 1.x provides content data records (CDR) backup capabilities for Cisco's Content Services Gateway (CSG). Release 2.0 adds CDR backup capabilities for the Cisco Gateway GPRS Serving Node (GGSN).

A single PSD can support both CSGs and GGSNs. The number of CSGs and GGSNs that can be supported by a single PSD is limited by the traffic load generated by each, as well as the duration of storage that you desire.

Storage and Retrieval on the PSD

Under normal conditions, a Cisco client will send content data records to Mediation Partners' servers. If those servers become unreachable—for any reason—records are then sent to the PSD for safekeeping until contact is re-established with the Charging Gateway (CG). Once contact is re-established, the client retrieves the records from the PSD, and forwards them to the CG.

Storage

Under normal conditions, the PSD provides backup capabilities when necessary—for example, during network outages. The PSD stores the payload from the packet in a queue, and is unaware of the content or format of that data, so that the data can be retrieved exactly as it was sent.

Retrieval

Once the client has determined that it's regular data server is reachable, you issue a CLI command to request that the data files for a given data store be transferred using FTP to a specified URL. You can also restore the configuration to a previously saved version that includes all the IP and application related configuration files. And, you can issue another CLI command to delete transferred files.

Note The GGSN requires all client Charging Gateways (CG) to send a Node Alive request when they initially startup. The GGSN uses receipt of the Node Alive as an indicator that a CG is now available. Therefore, the GTP' interface on the PSD supports sending Node Alive requests in order to properly support the GGSN.

Datastores

Datastores are locations for a particular client that map to the PSD's hard drive. In this release, you can create up to twenty (20) separate datastores and name them. Twenty datatstores support four MWAM cards in a single chassis with each running five client images, and allows each client to have its own data store. Additionally, datastores have access lists that you can configure to allow specific clients to read and write to specific datastores. Currently, the number of accessors is limited to two (2). The data store access list contains an optional port number in addition to the IP address for each accessor.

When the preferred destination for data becomes unavailable, or during any network outage, data is sent to the PSD and is stored on a "first come, first served" basis. The maximum record storage capability of the PSD is 37 gigabytes, and is allocated as needed.

Format of Datastore Data Files

A data store is comprised of one or more data files. Each data file is composed of multiple records that are constructed of various management related fields, data, and an end-of-record (EOR) indicator. If you need to retrieve data files using FTP (files that are usually corrupt), you will need to understand the format of the data. The following is the format for each record written to a data file:

Flag	CRC	Data Length	Data	EOR

- The "Flag" is a 4-byte integer value that indicates the status of the record. This value is used as a 32 bit mask with individual bits having specific meanings. The following bits have assigned values with bit 1 being the least significant (right most bit):
  - Bit 1: Record written—a value of "1" indicates that the record has been completely written to file. A value of "0" indicates that it is an incomplete record, and is probably corrupt.
  - Bit 2: Record acknowledged—a value of "1" indicates that the client has acknowledged that it read the record. A value of "0" indicates that the client has not acknowledged that it read the record.
  - Bit 3:CRC Present—a value of "1" indicates that the Circular Redundancy Check (CRC) field contains a CRC value for the data in this record. A value of "0" indicates the CRC field can be ignored when validating the record.
- The "CRC" is a 4-byte integer value representing a CRC-32 value.
- The "Data Length" is a 4-byte integer value representing the length of the Data field.
- The "Data" is the data the client device has written to the data store.
- The "EOR" is a one-byte value of 0xFF that indicates the end-of-record.

An End-of-File (EOF) marker follows the last record in a file. This marker is a 4 byte field with a value of 0xFFFFFFFF.

Data files are named with a numeric prefix and a file extension of ".data" (for example, 000000001.data).

Platform and Network Planning

In release 1.x and above, the PSD is implemented as a single linecard that sits in a Catalyst 6500 or 7600 chassis.

The PSD hardware supports the following features:

- Critical data backup from single failures
- Internal 40 GB hard disk, with a maximum storage capability of 37 GB.
- Single module in Catalyst 65xx or 76xx chassis

The typical configuration will be a chassis with up to twenty active co-resident clients and a single PSD serving those clients. The number of PSDs required is determined based on expected network traffic, and the corresponding records that Cisco clients would generate (for example, billing records from a CSG).

Cisco recommends that you consult your sales engineer for specific network planning. You can, however, get a general idea of how many PSDs your network requires by using the following criteria.

To determine the number of PSDs you need, take the maximum value of the following variables:

- Number of Clients ÷ the maximum number of Datastores per PSD, or
- Client transmit data rate ÷ the PSD's maximum receive data rate, or
- (Hours of storage × client transmit data rate) ÷ the max storage per PSD.

Additionally, the following values will be useful to you for network planning:

- Max datastores per PSD = 20
- Client transmit rate = 750MB per hour (actual rates will vary)
- PSD's max receive rate = 640MB per hour
- Max PSD storage capacity = 37GB

Configuring and Managing the PSD

The PSD is configured and managed by sessioning to the PSD module from IOS on the Supervisor card, or with Telnet when Telnet is enabled. The PSD is then configured using a CLI much like IOS. In addition to a number of administrative and troubleshooting commands on the PSD, there are basic configuration commands that allow you to create and manage datastores on the PSD, and to assign clients that may access (read/write) those datastores. Typically, you would configure a datastore for each client, or pair of redundant clients.

Additionally, you must configure the clients to inform them of the location and presence of a PSD.

New Features in Release 2.0

The following features are new for the PSD Release 2.0:

- The **configuration save** command is introduced to save and store PSD configuration files to a specified FTP URL.
- The **datatstore transfer** command is introduced to transfer PSD configuration files to a specified FTP URL, and to optionally delete them.
- The **configuration restore** command is introduced to restore a PSD using the saved configuration files from the specified FTP URL.

- The **datastore purge** command allows you to delete sets of files.
- The maximum number of data stores is increased to 20 (the equivalent to 4 MWAMs of GGSNs).
- The same PSD can be shared by a CSG and a GGSN.

PSD Features in Release 1.1(1)

These are the features for the Cisco PSD software release 1.1(1)

- Support for full capacity of the existing 40GB Hard drive, providing up to 37GB of record storage.

PSD Features in Release 1.0(1)

These are the features for the PSD in software release 1.0(1):

- The PSD supports up to 3 clients.
- Call Data Record Backup (CDRB) function to support the Cisco CSG.
- Data packets (CDRs) are retrievable in the order they were stored on the PSD.

Supported Platforms

- Catalyst 6500 Switch running IOS
- Cisco 7600 Internet Router running IOS

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Supported MIBs, and RFCs

The following sections provide information about the MIBs and RFCs that are supported on the PSD:

MIBs

- IF-MIB
- MIB-2
- HOST-RESOURCE-MIB

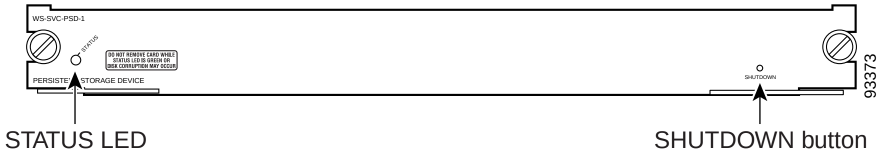
RFCs

- RFC1229—Manage network interfaces
- RFC1213—Standard network device management
- RFC1514, RFC2790—Detailed system resources management that provides the ability to see all processes and their utilization. Disk partitions are visible and disk usage is available. You need net-snmp agent for this support.

Front Panel Description

The PSD front panel (see Figure 1-1) includes a STATUS LED and SHUTDOWN button.

Figure 1-1 Persistent Storage Device Module


WS-SVC-PSD-1
STATUS
DO NOT REMOVE CARD WHILE STATUS LED IS GREEN OR DISK CORRUPTION MAY OCCUR
PERSISTENT STORAGE DEVICE
SHUTDOWN
93373
STATUS LED
SHUTDOWN button

STATUS LED

The STATUS LED indicates the operating states of the PSD. Table 1-1 describes the LED operation.

Table 1-1 STATUS LED Description

Color	Description
Green	All diagnostic tests pass. The PSD is operational.
Red	A diagnostic other than an individual port test failed.
Orange	Indicates one of three conditions: • The PSD is running through its boot and self-test diagnostic sequence. • The PSD is disabled. • The PSD is in the shutdown state.
Off	The PSD power is off.

SHUTDOWN Button

Push the “shutdown" buttom on the faceplate of the PSD card, then wait for the faceplate LED to change from green to amber.

Caution Do not remove the PSD from the switch until the PSD has shut down completely and the STATUS LED is off. You can corrupt data files, or you can damage the PSD if you remove it from the switch before it completely shuts down.

To avoid corrupting the PSD hard disk, you must correctly shut down the PSD before you remove it from the chassis or disconnect the power. This shutdown procedure is normally initiated by commands entered at the Supervisor engine CLI prompt or the PSD CLI prompt.

If the PSD fails to respond to these commands properly, you can use the SHUTDOWN button on the front panel to initiate the shutdown procedure.

The shutdown procedure may require several minutes. The STATUS LED turns orange when the PSD shuts down.

Conditions That Require Shutdown of a PSD Card

Before you perform any of the following operations, you should shut down the PSD:

- Physically remove the PSD cards from Cat6500/7600 slots.
- Manually switch the power off on the Cisco Catalyst 6500 or 7600 boxes.
- Any other conditions that causes a sudden power interruption of the chassis.

Methods to Shutdown the PSD Card

Use one of the following methods to gracefully power down the PSD cards:

- In SUP configuration mode, issue the **no power enable module** *mod #* command.
- In SUP exec mode, issue the **hw-module module** *mod #* **shutdown** command.
- Push the “shutdown" buttom on the faceplate of the PSD card.
- A software reload of the Supervisor IOS using the **reload** command in the Supervisor CLI (the whole box reloads).

Note If you use any other method to shutdown the PSD than the “shutdown” button, you must verify that the PSD is completely shutdown by looking at the state using the **show module** *n* command.

```
routert#sho mod  5
> Mod Ports Card Type                              Model              Serial No.
> --- ----- -------------------------------------- ------------------ -----------
>   5    3  Persistent Storage Device              WS-SVC-PSD-1       SAD10280323
>
> Mod MAC addresses                       Hw    Fw           Sw           Status
> --- ---------------------------------- ------ ------------ ------------ -------
>   5  0018.197e.22c2 to 0018.197e.22c9   3.0   7.2(1)       1.1(3)       ShutDown
```

Note Alternately, you can wait for the text “SP: PC shutdown completed for module 5” to appear on the console.

Specifications

Table 1-2 describes the specifications for the PSD.

Table 1-2 WS-SVC-PSD-1 Specifications

Specification	Description
Dimensions (H x W x D)	1.2 x 14.4 x 16 in. (3.0 x 35.6 x 40.6 cm)

Table 1-2 WS-SVC-PSD-1 Specifications (continued)

Specification	Description
Weight	Minimum: 3 lb (1.36 kg) Maximum: 5 lb (2.27 kg)
Environmental conditions:	
Operating temperature	32 to 104° F (0 to 40° C)
Nonoperating temperature	–40 to 158° F (–40 to 70° C)
Humidity	10 to 90%, noncondensing
Humidity - Ambient (Noncondensing) Nonoperating and Storage	5 to 95%
Altitude	Sea level to 10,000 ft (3050 m)

Safety Overview

Safety warnings appear throughout this document in procedures that may harm you if performed incorrectly.

For additional safety information, refer to documents listed in the “Related Documentation” section on page 1-51.

Warning

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.

Warning

WaarschuwingDit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het document *Regulatory Compliance and Safety Information* (Informatie over naleving van veiligheids- en andere voorschriften) raadplegen dat bij dit toestel is ingesloten.

Warning

VaroitusTämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. Tässä julkaisussa esiintyvien varoitusten käännökset löydät laitteen mukana olevasta *Regulatory Compliance and Safety Information* -kirjasesta (määräysten noudattaminen ja tietoa turvallisuudesta).

Warning **AttentionCe symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions d’avertissements figurant dans cette publication, consultez le document *Regulatory Compliance and Safety Information* (Conformité aux règlements et consignes de sécurité) qui accompagne cet appareil.**

Warning **WarnungDieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Dokument *Regulatory Compliance and Safety Information* (Informationen zu behördlichen Vorschriften und Sicherheit), das zusammen mit diesem Gerät geliefert wurde.**

Warning **AvvertenzaQuesto simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nel documento *Regulatory Compliance and Safety Information* (Conformità alle norme e informazioni sulla sicurezza) che accompagna questo dispositivo.**

Warning **AdvarselDette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du vare oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. Hvis du vil se oversettelser av deadvarslene som finnes i denne publikasjonen, kan du se i dokumentet *Regulatory Compliance and Safety Information* (Overholdelse av forskrifter og sikkerhetsinformasjon) som ble levert med denne enheten.**

Warning **AvisoEste símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. Para ver as traduções dos avisos que constam desta publicação, consulte o documento *Regulatory Compliance and Safety Information* (Informação de Segurança e Disposições Reguladoras) que acompanha este dispositivo.**

Warning **¡Advertencia!Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. Para ver una traducción**

de las advertencias que aparecen en esta publicación, consultar el documento titulado *Regulatory Compliance and Safety Information* (Información sobre seguridad y conformidad con las disposiciones reglamentarias) que se acompaña con este dispositivo.

Warning **Varning!Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du varamedveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. Se förklaringar av de varningar som förkommer i denna publikation i dokumentet *Regulatory Compliance and Safety Information* (Efterrättelse av föreskrifter och säkerhetsinformation), vilket medföljer denna anordning.**

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.**

Software Requirements

Table 1-3 lists the PSD software versions supported by Cisco IOS software.

Table 1-3 PSD Software Compatibility

Application Image	Maintenance Image	Cisco IOS Software	Cisco Client Software
2.0	2.1(2)	12.2(17d)SXb or later	PSD Release 2.0 supports CSG release 3.1(3)C4(1) and later, and GGSN release 6.0.
1.1(1) through 1.1(4)	1.4(1)m	12.2(14)ZA2 or later releases with a Supervisor Engine 2 with an MSFC2	PSD Release 1.1(1) supports CSG release 3.1(3)C4(1)

Hardware Requirements

Table 1-4 lists the PSD hardware versions supported by Cisco IOS software.

Table 1-4 PSD Supported Hardware Version

Cisco IOS Software
Supervisor Engine 2 with an MSFC2 or Supervisor 720 with an MSFC3

Required Tools

Note Before installing the PSD, you must install the Catalyst 6500 series switch chassis, and at least one Supervisor engine. For information on installing the switch chassis, refer to the *Catalyst 6000 Family Installation Guide*.

These tools are required to install the PSD in the Catalyst 6500 series switch:

- Flat-blade screwdriver
- Phillips-head screwdriver
- Wrist strap or other grounding device
- Antistatic mat or antistatic foam

Whenever you handle the PSD, always use a wrist strap or other grounding device to prevent electrostatic discharge (ESD).

Installing and Removing the PSD

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.**

All the Catalyst 6500 series family switches support hot swapping, which allows you to install, remove, replace, and rearrange modules without turning off the system power. For more information on removing the PSD from a switch, see the "Removing a Module" section on page 1-12.

Caution Do not remove the PSD from the switch until the PSD has shut down completely and the STATUS LED is orange. You can corrupt data files, or damage the PSD if you remove it from the switch before it completely shuts down.

When the system detects that a module has been installed or removed, the system automatically runs diagnostic and discovery routines, acknowledges the presence or absence of the module, and resumes system operation.

To install and use the PSD, you need to complete the following actions:

- Perform the initial installation by placing the PSD in a switch.
- At the switch CLI, session to the PSD CLI and provide a basic configuration.
- Test network conncectivity by pinging an external client.

This section describes how to install and verify the operation of the PSD in the Catalyst 6500 family switch, and contains the following sections:

- Slot Assignments, page 1-12
- Removing a Module, page 1-12
- Installing a Module, page 1-13
- Verifying the Installation, page 1-21

Slot Assignments

The Catalyst 6509 switch chassis has nine slots. The module can occupy any slot in the Catalyst 6500 series chassis.

Note The Catalyst 6509-NEB switch has vertical slots numbered 1 to 9 from right to left. Install the modules with the component side facing to the right.

- Slot 1 is reserved for the Supervisor engine.
- Slot 2 can contain an additional redundant Supervisor engine in case the Supervisor engine in slot 1 fails.
- If a redundant Supervisor engine is not required, slots 2 through 6 on the 6-slot chassis, (slots 2 through 9 on the 9-slot chassis and slots 2 through 13 on the 13-slot chassis) are available for switching modules, or other application modules.
- Install switching-module filler plates, which are blank switching-module carriers, in the empty slots to maintain consistent airflow through the switch chassis.

Removing a Module

This section describes how to remove an existing module from a chassis slot.

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.**

Warning **Before you install, operate, or service the system, read the *Site Preparation and Safety Guide*. This guide contains important safety information you should know before working with the system.**

Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.**

To remove a Supervisor engine or module from the chassis, perform these steps:

Step 1 Disconnect any network interface cables attached to the Supervisor engine or module.

Note The PSD does not have any interface cable connections. It communicates throught the chassis backplane.

Step 2 Verify that the captive installation screws on all of the modules in the chassis are tight.

This action ensures that the space created by the removed module is maintained.

Note If the captive installation screws are loose, the electromagnetic interference (EMI) gaskets on the installed modules will push the modules toward the open slot, reducing the opening size and making it difficult to install the replacement module.

Step 3 Loosen the two captive installation screws on the Supervisor engine or module.

Step 4 Depending on the orientation of the slots in the chassis (horizontal or vertical), perform one of the following sets of steps:

Horizontal slots

a. Place your thumbs on the left and right ejector levers, and simultaneously rotate the levers outward to unseat the module from the backplane connector.

b. Grasp the front edge of the module and slide the module part of the way out of the slot. Place your other hand under the module to support the weight of the module. Do not touch the module circuitry.

Vertical slots

a. Place your thumbs on the ejector levers located at the top and bottom of the module, and simultaneously rotate the levers outward to unseat the module from the backplane connector.

b. Grasp the edges of the module, and slide the module straight out of the slot. Do not touch the module circuitry.

Step 5 Place the module on an antistatic mat or antistatic foam, or immediately reinstall it in another slot.

Step 6 If the slot is to remain empty, install a module filler plate to keep dust out of the chassis and to maintain proper airflow through the chassis.

Warning **Blank faceplates (filler panels) serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards and faceplates are in place.**

Installing a Module

This section describes how to install modules in the Catalyst 6500 series and Catalyst 6000 family switches.

Caution To prevent ESD damage, handle modules by the carrier edges only.

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.**

Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.**

Warning **Before you install, operate, or service the system, read the *Site Preparation and Safety Guide*. This guide contains important safety information you should know before working with the system.**

To install a Supervisor engine or module in the chassis, perform these steps:

Step 1 Choose a slot for the Supervisor engine or module.

Step 2 Verify that there is enough clearance to accommodate any interface equipment that you will connect directly to the Supervisor engine or module ports. If possible, place modules between empty slots that contain only module filler plates.

Step 3 Verify that the captive installation screws are tightened on all modules installed in the chassis.

This action ensures that the EMI gaskets on all modules are fully compressed in order to maximize the opening space for the new module or the replacement module.

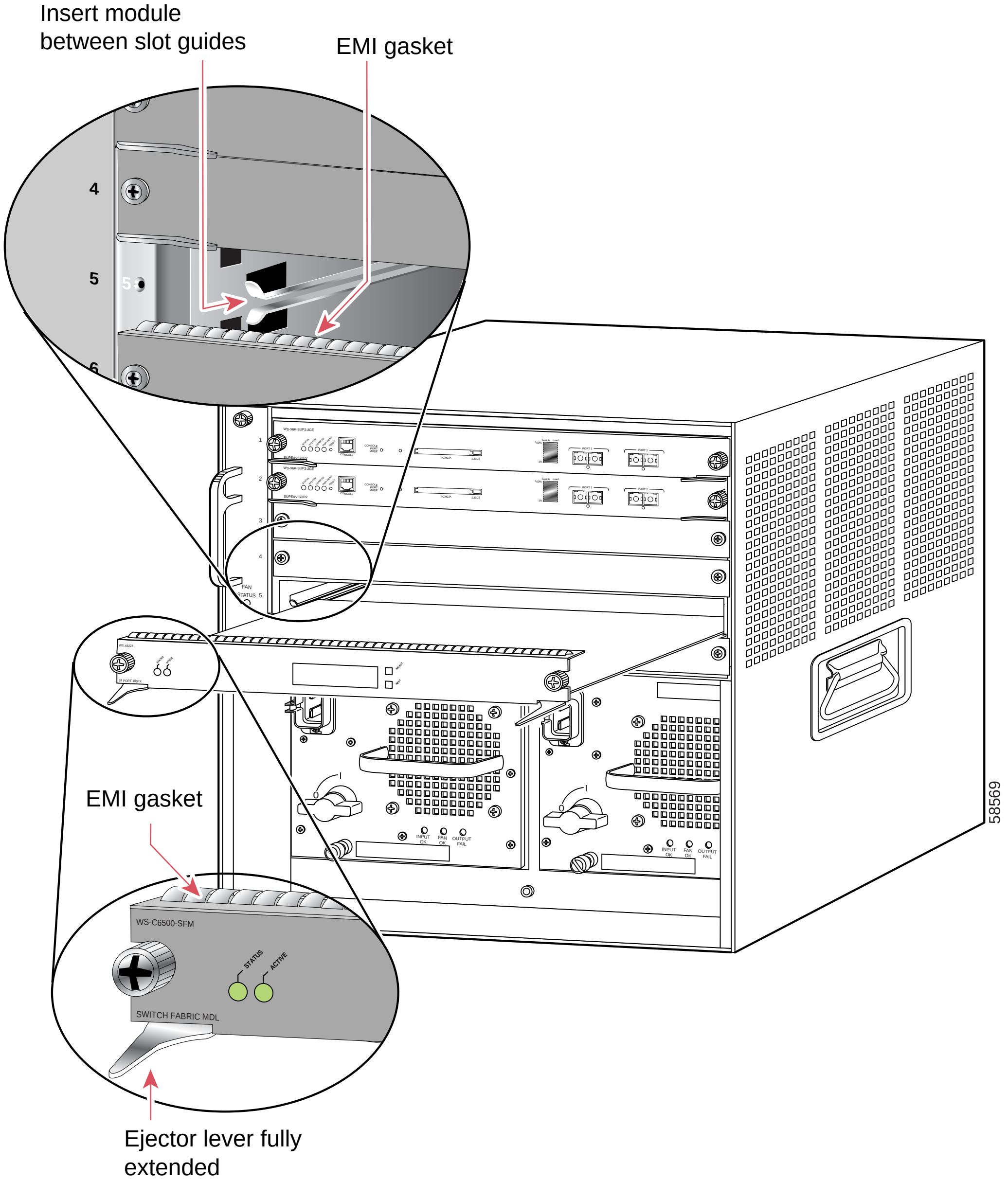
Note If the captive installation screws are loose, the EMI gaskets on the installed modules will push adjacent modules toward the open slot, reducing the opening size and making it difficult to install the replacement module.

Step 4 Remove the module filler plate by removing the two Phillips pan-head screws from the filler plate.

To remove a module, refer to "Removing a Module" section on page 1-12.

Step 5 Fully open both ejector levers on the new or replacement module. (See Figure 1-2.)

Figure 1-2 Positioning the Module in a Horizontal Slot Chassis



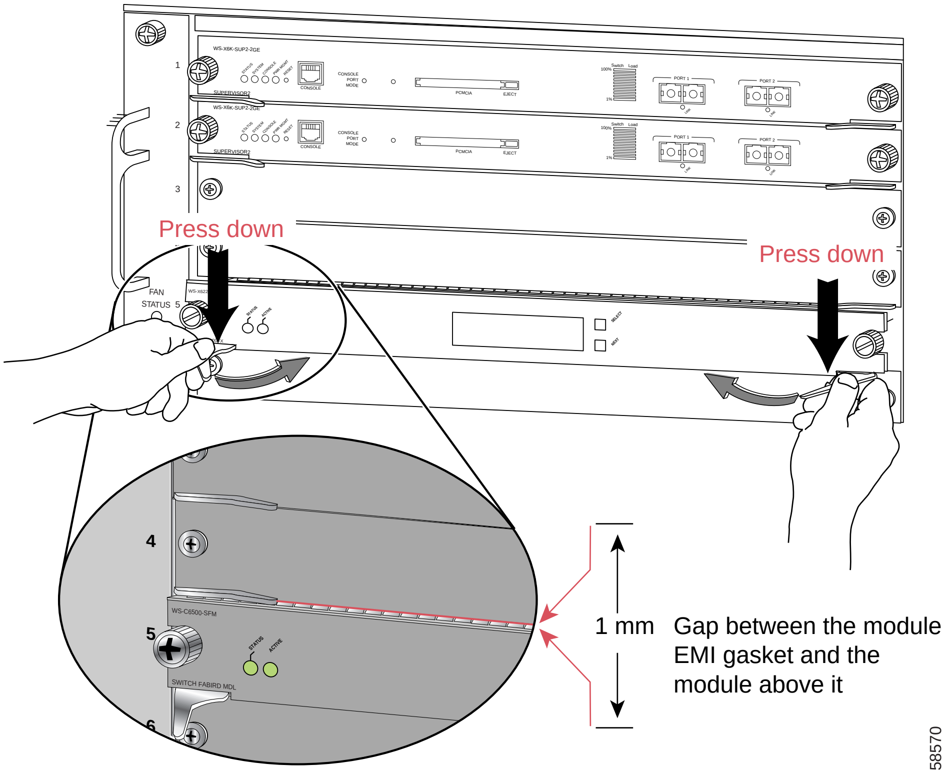
Step 6 Depending on the orientation of the slots in the chassis (horizontal or vertical), perform one of these sets of steps:

Horizontal slots

a. Position the Supervisor engine or module in the slot. (See Figure 1-2.) Make sure that you align the sides of the module carrier with the slot guides on each side of the slot.

b. Carefully slide the Supervisor engine or module into the slot until the EMI gasket along the top edge of the module makes contact with the module in the slot above it and both ejector levers have closed to approximately 45 degrees in relation to the module faceplate. (See Figure 1-3.)

Figure 1-3 Clearing the EMI Gasket in a Horizontal Slot Chassis

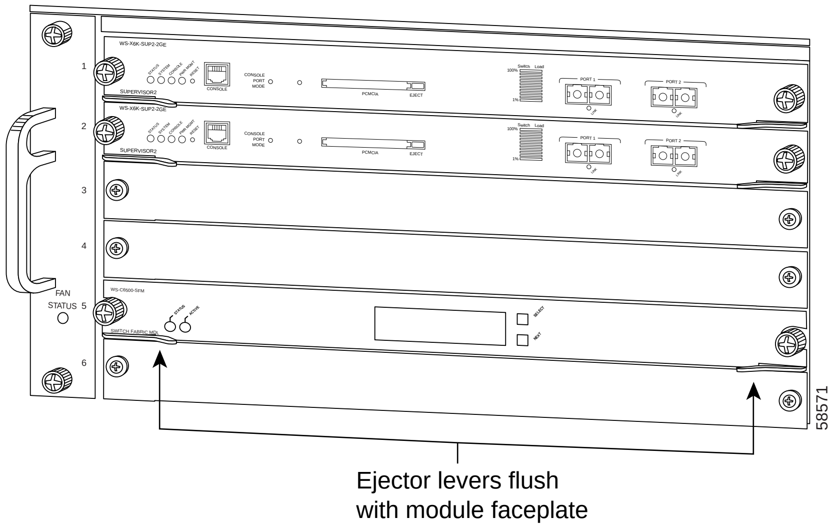


c. Using the thumb and forefinger of each hand, grasp the two ejector levers and press down to create a small (0.040 inch [1 mm]) gap between the module's EMI gasket and the module above it. (See Figure 1-3.)

Caution Do not press down too hard on the levers because they can bend and be damaged.

d. While pressing down, simultaneously close the left and right ejector levers to fully seat the Supervisor engine or module in the backplane connector. The ejector levers are fully closed when they are flush with the module faceplate. (See Figure 1-4.)

Figure 1-4 Ejector Lever Closure in a Horizontal Slot Chassis



Note Failure to fully seat the module in the backplane connector can result in error messages.

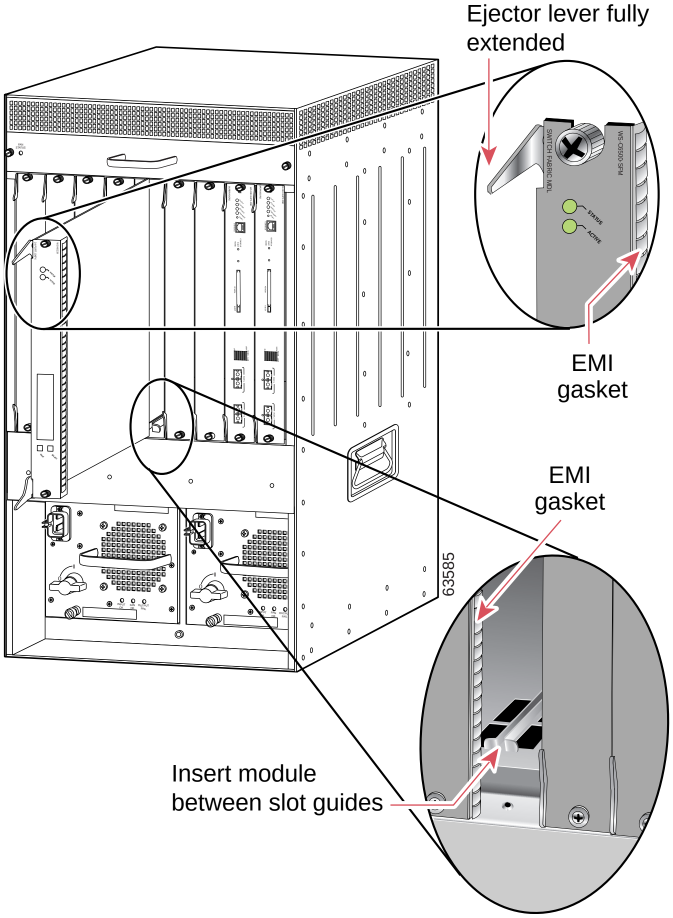
e. Tighten the two captive installation screws on the Supervisor engine or module.

Note Make sure that the ejector levers are fully closed before tightening the captive installation screws.

Vertical slots

a. Position the Supervisor engine or switching module in the slot. (See Figure 1-5.) Make sure that you align the sides of the switching module carrier with the slot guides on the top and bottom of the slot.

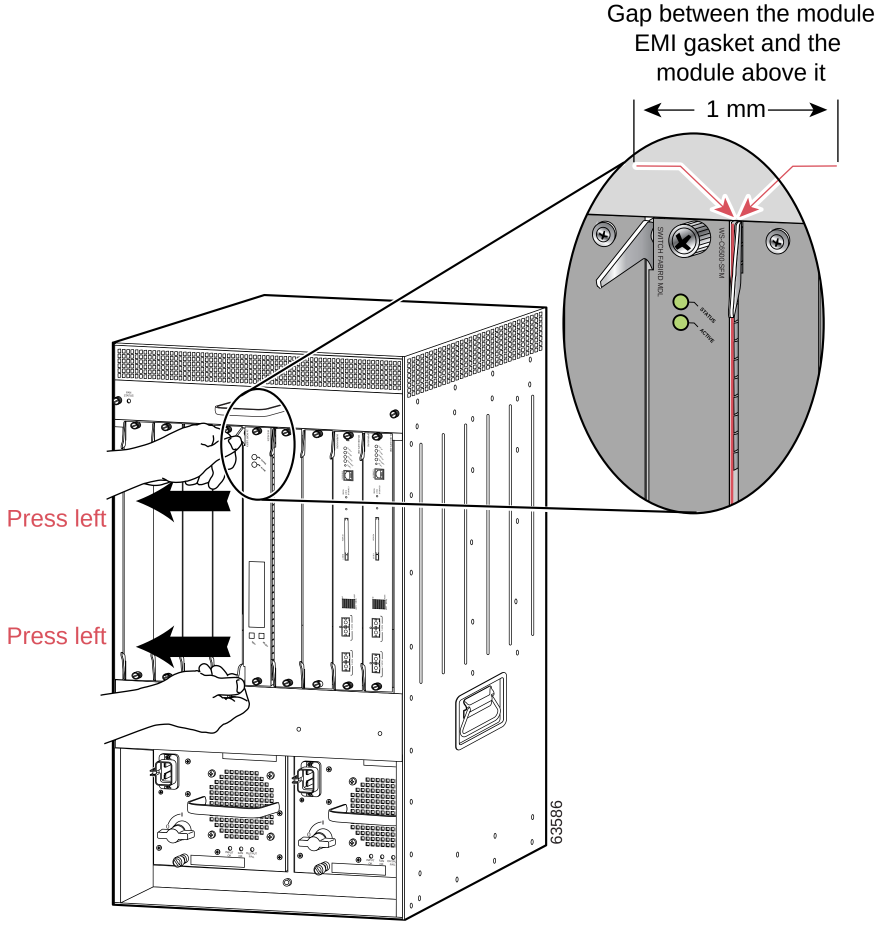
Figure 1-5 Positioning the Module in a Vertical Slot Chassis



b. Carefully slide the Supervisor engine or module into the slot until the EMI gasket along the right edge of the module makes contact with the module in the slot adjacent to it and both ejector levers have closed to approximately 45 degrees with respect to the module faceplate. (See Figure 1-6.)

c. Using the thumb and forefinger of each hand, grasp the two ejector levers and exert a slight pressure to the left, moving the module approximately 0.040 inches (1 mm) to create a small gap between the module's EMI gasket and the module adjacent to it. (See Figure 1-6.)

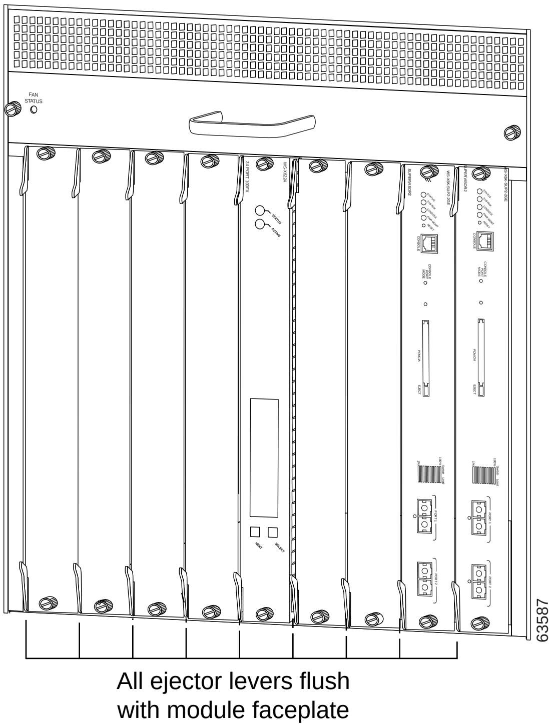
Figure 1-6 Clearing the EMI Gasket in a Vertical Slot Chassis



Caution Do not exert too much pressure on the ejector levers. They will bend and be damaged.

d. While pressing on the ejector levers, simultaneously close them to fully seat the Supervisor engine or module in the backplane connector. The ejector levers are fully closed when they are flush with the module faceplate. (See Figure 1-7.)

Figure 1-7 Ejector Lever Closure in a Vertical Slot Chassis



e. Tighten the two captive installation screws on the module.

> **Note** Make sure that the ejector levers are fully closed before tightening the captive installation screws.

Note For information regarding installation details for the Cisco 7600 Internet Router, go to the following URL:
http://www.cisco.com/en/US/products/hw/routers/ps368/products_module_installation_guide_book09186a008007cd9d.html

Verifying the Installation

This section describes how to verify the PSD installation.

Cisco IOS Software

To verify that the system acknowledges the new module and has brought it online, enter the **show module** [*mod-num* | **all**] command.

This example shows the output of the **show module** command:

```
Router#show module
Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  1    2  Catalyst 6000 supervisor 2 (Active)    WS-X6K-SUP2-2GE    SAL06396QLA
  2    2  Catalyst 6000 supervisor 2 (Standby)   WS-X6K-SUP2-2GE    SAL061800UB
  3   48  48 port 10/100 mb RJ45                 WS-X6348-RJ-45     SAL06200V6W
  4    3  Network Analysis Module                WS-SVC-NAM-1       SAD064403UB
  5    3  Persistent Storage Device              WS-SVC-PSD-1       SAD060301SU
  6    3  Persistent Storage Device              WS-SVC-PSD-1       SAD060301SV

Mod MAC addresses                       Hw     Fw           Sw           Status
--- ---------------------------------- ------ ------------ ------------ -------
  1  0006.d65b.e1bc to 0006.d65b.e1bd   3.10   6.1(3)       7.5(0.94)    Ok
  2  0005.7485.bde8 to 0005.7485.bde9   3.7    6.1(3)       7.5(0.94)    Ok
  3  0009.1243.23cc to 0009.1243.23fb   6.1    5.4(2)       7.5(0.94)    Ok
  4  0002.7ee4.b046 to 0002.7ee4.b04d   1.0    7.2(1)       2.2(1a)      Ok
  5  00e0.b0ff.3630 to 00e0.b0ff.3637   0.101 7.5(0.61)     1.0(1)       Ok
  6  00e0.b0ff.3530 to 00e0.b0ff.3537   0.101 7.5(0.61)     1.0(1)       Ok

Mod Sub-Module                  Model           Serial           Hw     Status
--- --------------------------- --------------- --------------- ------- -------
  1 Policy Feature Card 2       WS-F6K-PFC2     SAL06396LVK      3.3    Ok
  1 Cat6k MSFC 2 daughterboard  WS-F6K-MSFC2    SAL06365RJM      2.5    Ok
  2 Policy Feature Card 2       WS-F6K-PFC2     SAL061735WF      3.2    Ok
  2 Cat6k MSFC 2 daughterboard  WS-F6K-MSFC2    SAL06131NAL      2.3    Ok

Mod Online Diag Status
--- -------------------
  1 Pass
  2 Pass
  3 Pass
  4 Pass
  5 Pass
  6 Pass
```

When the PSD initially boots, by default it runs a partial memory test. To perform a full memory test, enter the **hw-module module** *module_number* **reset** *device:partition* **mem-test-full** command.

A full memory test takes more time to complete than a partial memory test depending on the memory size. Table 1-5 lists the memory test time and approximate boot time for a partial memory test.

Table 1-5 Module Boot Time

Module	Boot Time
WS-SVC-PSD-1	9 minutes

You also can use the **hw-module module** *module_number* **mem-test-full** command in a Cisco IOS system. This example shows how to do a full memory test for module 4:

```
Router(config)#  hw-module module 4 mem-test-full
```

Note Cisco recommends that you run a full online diagnostic when you boot your PSD for the first time. You can use the following commands to perform this task:

```
router# configure terminal diag level complete
```

Configuring the PSD

See the following sections for configuration tasks for the PSD. Each task in the list is identified as either required or optional.

- Configuring the Supervisor for the PSD, page 1-23
- "Adding the PSD to the Corresponding VLAN" section on page 1-23
- "Initial PSD Configuration" section on page 1-23
- "Transfering and Purging Data Files and Datastores" section on page 1-27
- "Administering the PSD" section on page 1-27

There are several external interfaces that are available to configure and manage the PSD. They include the following:

MP (Maintenance Partition) Command Line Interface.

When you boot the MP image (from compact flash), and login to the card, you are presented with a command line interface that allows you to perform activities such as administration tasks, configuration, troubleshooting, and to upgrade the application image.

AP (Application Partition) Command Line Interface.

When you boot the AP image from the hard disk, and login to the card, you are presented with a command line interface that is similar to IOS. The AP commands allow you to configure the PSD, and to display the status of the PSD.

There is a specific subset of the PSD CLI commands for the following tasks:

- Taking the PSD into service
- Taking the PSD out of service
- Creating a data store for a client
- Deleting a data store
- Showing PSD related status and datastore information
- Enabling access to a datastore
- Disabling access to a datastore

IOS Supervisor Command Line Interface.

This is the command line provided by the IOS image on the Supervisor card. There are IOS commands that allow you to interact with the PSD card. The Supervisor CLI also provides commands by which the CSG or GGSN is configured to communicate with the PSD card.

SNMP interfaces. The SNMP agent on the PSD can be configured and activated. When activated, you can then define a read community string. A network agent with connectivity to the PSD, and knowledge of the SNMP read community string, may issue SNMP get/walk type requests to manage and monitor the PSD.

Configuring the Supervisor for the PSD

Adding the PSD to the Corresponding VLAN

By default, the PSD is in trunking mode with native VLAN 1.

Note By default the PSD will use vlan1 for its network traffic; however, you can configure the PSD to use another vlan with the **persistent-store module** command.

Initial PSD Configuration

Before you can use the PSD for data storage, you must log into the PSD root account and configure the following:

- IP address
- Subnet mask
- IP broadcast address
- IP host name
- Default gateway
- Domain name
- Datastore Creation and Access Control
- Inservice
- If applicable, the DNS name server
- If you are using an external SNMP manager to communicate with the PSD, configure the following:
  - SNMP MIB variables
  - Access control for the SNMP agent
  - System group settings on the PSD

To configure these required parameters for the PSD, follow these steps:

Step 1 Enter this command to verify that the PSD is installed and that the power is on:

```
Router#  show module mod
```

Step 2 Establish a console session with the PSD by entering:

```
Router#  session slot module_number processor 1
```

Note Sometimes attempts to session into the PSD console from the supervisor fail immediately after startup, or immediately after a PSD restart, even though the “module online” message for the PSD blade has appeared at the supervisor. Always wait 60 seconds after the "module online" message appears on the supervisor for the PSD module before you attempt to session into the PSD from the supervisor.

The hardware and firmware of the PSD performs self-checks on boot up, then notifies the supervisor that the PSD module is online. This results in the “module online” message at the supervisor console. Concurrently, the firmware starts the PSD application on the PSD processors. The PSD application requires about 50 seconds to initialize itself, and the application does not accept session requests from the supervisor until this initialization is complete.

Step 3 At the login prompt, type **root** to log in to the root account.

Step 4 At the password prompt, type **cisco** as the root password.

Note If you have not changed the password from the factory-set default, a warning message displays. If you decide to change the password from the default, see the “Changing the PSD CLI Passwords” section on page 1-29 for more information.

Step 5 Configure the IP address and subnet mask by entering:

```
root@localhost# ip address ip-address subnet-mask
```

Step 6 Configure the IP broadcast address by entering:

```
root@localhost# ip broadcast broadcast-address
```

Step 7 Configure the IP host name used in the CLI prompt, **show** commands, and log messages by entering:

```
root@localhost# ip host [host-name]
```

Step 8 Configure the default gateway by entering:

```
root@localhost# ip gateway default-gateway
```

Note This gateway should always be the IP address of VLAN1 on the Supervisor.

Step 9 Configure the domain name for the PSD by entering:

```
root@localhost# ip domain domain-name
```

Step 10 Configure one or more IP addresses as DNS name servers by entering:

```
root@localhost# ip nameserver ip-address [ip-address2] [ip-address-3]
```

Note The **ip nameserver** command can accept up to a maximum of three name server addresses (two addresses are optional).

Step 11 Verify the PSD configuration by entering:

```
root@localhost# show ip
```

Step 12 Configure a datastore for a Cisco client by entering:

```
root@localhost# datastore create cisco
root@localhost# datastore access enable cisco 1.2.3.4 port number
root@localhost# show datastore all or cisco
```

Step 13 Put the PSD inservice by entering:

```
root@localhost# in-service
```

Note The following steps are optional configuration tasks:

Step 14 Configure the SNMP syslocation MIB variable by entering:

```
root@localhost# snmp-agent location-string
```

Note The MIB variables in Step 13 and Step 14 must be valid DisplayString texts, each with a maximum length of 64 characters.

Step 15 Set the SNMP sysContact MIB variable by entering:

```
root@localhost# snmp-contact contact-string
```

Step 16 Set the SNMP sysName MIB variable by entering:

```
root@localhost# snmp-name name-string
```

Note You can delete the SNMP location, SNMP contact, or SNMP name by entering the respective command without any parameters.

Step 17 Set the SNMP agent community string parameter password for read-write access by entering:

```
root@localhost# snmp-community community-string
```

Note Clear the SNMP community string with the **snmp delete community** command.

Step 18 Verify the SNMP access controls and settings by entering:

```
root@localhost# show snmp
```

Step 19 Enable telnet access to your PSD module from a remote location by entering:

```
root@localhost# telnet-server enable
```

After completing this configuration, the PSD is ready to use with other Cisco clients.

This example shows how to configure the PSD:

```
Router#  session slot 8 processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.81 ... Open

Cisco Persistent Storage (WS-SVC-PSD-1)
```

```
login: root
Password:

Cisco Persistent Storage Device (WS-SVC-PSD-1) Console, 1.0(1)
Copyright (C) 2002-2003 by cisco Systems, Inc.

WARNING! Default password has not been changed!

root@localhost.localdomain# ip address 192.18.12.221 255.255.255.192
root@localhost.localdomain# ip host psd1
root@psd1.localdomain# ip gateway 192.18.12.193
root@psd1.localdomain# ip domain cisco.com
root@psd1.cisco.com# ip nameserver 161.44.11.21
root@psd1.cisco.com# show ip
IP address:         192.18.12.221
Subnet mask:        255.255.255.192
IP Broadcast:       192.18.255.255
DNS Name:           psd1.cisco.com
Default Gateway:    192.18.12.193
Nameserver(s):      161.44.11.21
FTP Server:         disabled
Telnet Server:      disabled
root@psd1.cisco.com# snmp-agent enable
root@psd1.cisco.com# snmp-agent community read
root@psd1.cisco.com# snmp-agent location "Cisco Lab, Building 10 Lab 4"
root@psd1.cisco.com# snmp contact "Lab Admin, 555-1212"
root@psd1.cisco.com# show snmp-agent
SNMP Agent:         psd1.cisco.com
status:             enabled
ip address:         172.18.12.221
community string:   read
SNMPv1:             supported
SNMPv2c:            supported
SNMPv3:             not-supported
sysDescr:           Linux psd1.cisco.com 2.4.18 #1 SMP Wed Jul 16 11:18:19 EDT 2
003 i686
sysObjectID:        OID: enterprises.ucdavis.ucdSnmpAgent.linux
sysContact:         Lab Admin, 555-1212
sysName:            not-configured
sysLocation:        Cisco Lab, Building 10 Lab 4
root@psd1.cisco.com#
```

Caution The PSD does not provide a dynamic method to save and restore your configuration. Additionally, if you need to change PSD modules in the Catalyst chassis, you will need to configure the new module. Cisco recommends that you perform the following procedure to save and store your PSD configuration details:

Step 1 Session into the PSD:

```
router# session slot slot_num processor processor
```

Step 2 Issue the **configuration save** command.

Note You can also issue the following **show** commands, and copy and paste the various **show** output into your preferred text editor:
root@localhost.localdomain# **show ip**
root@localhost.localdomain# **show snmp-agent**
root@localhost.localdomain# **show datastore all** .
Save this file in a secure location for backup purposes.

Note For specific information on how to configure the PSD to communicate with the CSG, refer to the "PSD Configuration for Content Services Gateway" chapter in the *Cisco Content Service Gateway Installation and Configuration Guide*.

Transfering and Purging Data Files and Datastores

The PSD allows you transfer and purge whole datastores, as well as individual files that exist in a datastore. See Troubleshooting the PSD, page 1-43 for more information about how to identify corrupt data files.

To transfer and purge datastores and datastore files, perform the following procedure:

Step 1 Issue the **datatstore transfer** command to push files to a designated URL using FTP. You can keep or delete all data files, all salvage files, or all files. Here is the syntax:

```
datastore transfer {keep | delete} {data-files | salvage-files | all} data-store-name
ftp-url
```

The specified URL has the following format:
ftp://*username*:*password@hostname*/*fully-qualified-destination-directory*

Step 2 After you have transferred data and/or salvage files to an FTP server, you can purge specific files of a datastore by issuing the datastore purge command. You can purge data files, salvage files, or all files. Here is the syntax:

```
datastore purge transferred {data-files | salvage-files | all} data-store-name
```

Administering the PSD

This section contains the various administrative tasks you can perform on the PSD with Cisco IOS:

- Logging in to the PSD, page 1-28
- Changing the PSD CLI Passwords, page 1-29
- Resetting the PSD, page 1-30
- Upgrading the PSD Software, page 1-30

Logging in to the PSD

Note The PSD has one user level "root". The default password is "cisco".

Table 1-6 shows the user levels and passwords for the PSD's Application Partition.

Table 1-6 Application Image Password

Application Image (located on the hard disk)	
User	**Password**
root	cisco

Table 1-7 shows the user levels and passwords for the PSD's Application Partition.

Table 1-7 PSD Users and Passwords for the MP

Maintenance Image (located on the compact flash)	
User	**Password**
root	cisco
guest	cisco

Note The guest account in the PSD maintenance image has "All Read" and "All Write" privileges. On the application image, the root user has full access and there is no "guest" account.

When you boot into either the application image or the maintenance image and set up IP information, that information is synched between the images. However, if you change passwords, that information is not synched between the images, and is not reflected on the unchanged image.

To allow remote Telnet sessions, use the **telnet-server enable** command.

To log in to the PSD, follow these steps:

Step 1 Log in to the Catalyst 6500 switch using the Telnet connection or the console port connection.

Step 2 At the CLI prompt, establish a console session with the PSD using the **session slot** *slot_number* **processor 1** command, as follows:

```
Router# session slot 8 processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.81 ... Open

Persistent Storage Module (WS-SVC-PSD-1)
```

Step 3 At the PSD login prompt, type **root** to log in as the root user or **guest** to log in as a guest user.

```
login: root
```

Step 4 At the password prompt, enter the password for the account. The default password for the root account is “cisco” and the default password for the guest account is “cisco”.

```
Password:
```

After a successful login, the command line prompt appears as follows:

```
Persistent Storage Module (WS-SVC-PSD-1) Console, 1.0(1)
Copyright (c) 1999-2002 by cisco Systems, Inc.

WARNING! Default password has not been changed!

root@localhost#
```

Changing the PSD CLI Passwords

If you have not changed the password from the factory-set default, a warning message displays when you log in to the PSD.

Note New passwords must be at least six characters in length, and may include uppercase and lowercase letters, numbers, and punctuation marks.

Note If the PSD maintenance image passwords are lost for the root or guest account, the maintenance image must be upgraded. After the upgrade, the passwords are set to the default. See Table 1-6 on page 1-28.

To change the password, follow these steps while you are logged in to the root account on the PSD:

Step 1 Enter this command:

```
root@localhost# password username
```

To change the root password, make a Telnet connection to the PSD and use the **password root** command.

To change the guest password in MP mode only, make a Telnet connection to the PSD and use the **password guest** command.

Step 2 Enter the new password:

```
Changing password for user root
New UNIX password:
```

Step 3 Enter the new password again:

```
Retype new UNIX password:
passwd: all authentication tokens updated successfully
```

This example shows how to set the password for the root account:

```
root@localhost# password root
Changing password for user root
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully
```

If you forget or lose the password, you can enter the **clear module pc-module** *module number* **password** command from the IOS Supervisor CLI to restore the password for the root account to "cisco".

Resetting the PSD

If you cannot reach the PSD through the CLI or an external Telnet session, enter the **hardware_module module module_number reset** command to reset and reboot the PSD. The reset process requires several minutes.

When the PSD initially boots, by default it runs a partial memory test. To perform a full memory test, use the **mem-test-full** keyword in the **hw-module module** *module_number* **reset** *device:partition* **mem-test-full** command.

When you next reset the PSD, the full memory test runs. A full memory test takes more time to complete than a partial memory test. See Table 1-5 for memory test times.

You can also use the **hw-module module** *module_number* **mem-test-full** configuration to run a memory test. This example shows a full memory test for module 5:

```
Router(config)#  hw-module slot 5 memory test full
```

To reset the module from the CLI, perform this task in privileged mode:

Task	Command
Reset the module.	**hw-module module** *mod_num* **reset device:** *partition* **mem-test-full** The device: *partition* value is the string for PC boot device, for example: **hdd:x** designates the hard disk, **cf:x** designates the compact Flash where **x** is the number for the partition on each device.

This example shows how to reset the PSD that is installed in slot 9 from the CLI:

```
Router# hardware_module mod 9 reset cf:1 memtest-full

Proceed with reload of module? [confirm] y
% reset issued for module 9
```

Note For the boot device, you can specify hdd:1 for the application image or cf:1 for the maintenance image.

Upgrading the PSD Software

You can upgrade both the application software and the maintenance software. To upgrade the application software, see the "Upgrading the PSD Application Software" section on page 1-34. To upgrade the maintenance software, see the "Upgrading the PSD Maintenance Software" section on page 1-31.

Caution If you are upgrading from Release 1.0(x) to Release 1.1(1), you will lose all existing data because the hard drive must be repartitioned to enable the PSD to use of the additional 20GB of disk space. If you perform a normal upgrade, the IP and data store configurations will be preserved; however, if you perform an upgrade and specify the "-install" option, you will lose your data and data store configurations.

Note Upgrading from Release 1.x to 2.0 will preserve data when you upgrade without the "-install" option.

Upgrading the PSD Maintenance Software

Note In the event that you need to upgrade your MP image, refer to the following URL for image location: http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-serv-maint

To upgrade the PSD maintenance software, follow these steps:

Step 1 Copy the PSD maintenance software image to a directory accessible to FTP.

Step 2 Log in to the switch through the console port or through a Telnet session.

Step 3 If the PSD is running in the application image go to Step 4. If the PSD is not running in the application image, enter this command in the privileged mode:

```
Router# hardware_module module 9 reset
Device BOOT variable for reset = hdd:1
Warning:Device list is not verified.

Proceed with reload of module? [confirm]
% reset issued for module 9
Router#
00:31:11:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:31:11:SP:The PC in slot 9 is shutting down. Please wait ...
00:31:25:SP:PC shutdown completed for module 9
00:31:25:%C6KPWR-SP-4-DISABLED:power to module in slot 9 set off (admin
request)
00:31:28:SP:Resetting module 9 ...
00:31:28:%C6KPWR-SP-4-ENABLED:power to module in slot 9 set on
00:33:26:%SNMP-5-MODULETRAP:Module 9 [Up] Trap
00:33:26:%DIAG-SP-6-BYPASS:Module 9:Online Diagnostics is Bypassed
00:33:26:%OIR-SP-6-INSCARD:Card inserted in slot 9, interfaces are now
online
```

Step 4 After the PSD is back online, establish a console session with the PSD and log in to the root account.

Step 5 Upgrade the PSD maintenance software by entering:

```
root@localhost# upgrade ftp-url
```

ftp-url is the FTP location and name of the PSD software image file.

Note If the FTP server does not allow anonymous users, use the following syntax for the *ftp-url* value: ftp://user@host/absolute-path/filename. Enter your password when prompted.

Step 6 Follow the screen prompts during the upgrade.

Step 7 After completing the upgrade, log out of the PSD.

Step 8 Boot into the maintenance image with the following command to reset the PSD maintenance software:

```
Router# hardware_module module 9 reset cf:1
Device BOOT variable for reset = cf:1
Warning:Device list is not verified.

Proceed with reload of module? [confirm]
% reset issued for module 9

Router#
00:16:06:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:16:06:SP:The PC in slot 9 is shutting down. Please wait ...
00:16:21:SP:PC shutdown completed for module 9
00:16:21:%C6KPWR-SP-4-DISABLED:power to module in slot 9 set off (admin
request)
00:16:24:SP:Resetting module 9 ...
00:16:24:%C6KPWR-SP-4-ENABLED:power to module in slot 9 set on
00:18:21:%SNMP-5-MODULETRAP:Module 9 [Up] Trap
00:18:21:%DIAG-SP-6-BYPASS:Module 9:Online Diagnostics is Bypassed
00:18:21:%OIR-SP-6-INSCARD:Card inserted in slot 9, interfaces are now
online
Router#
```

Step 9 (Optional) Verify the initial configuration after the PSD comes back online by logging into the PSD root account and enter the following command:

```
root@localhost# show ip
```

Step 10 Upgrade the Bios using the following commands:

a. Boot the PSD to the MP.

b. At the login prompt enter **guest**.

c. At the password prompt enter **cisco**.

d. Enter router# **hw-module module** *module_number* **cf:1**

e. Session to the PSD from the switch CLI.

f. Issue the **session slot** *module_number* **proc 1** command.

g. Enter **upgrade-bios** and follow the prompts

h. Enter the following Bios file name: **B01MQ009.ROM**

Step 11 (Optional) Reboot into the application image by entering:

```
Router# hardware_module module 9 reset
```

This example shows how to upgrade the PSD maintenance software:

```
Router#
Router# hardware_module module 9 reset
Device BOOT variable for reset = hdd:1
Warning:Device list is not verified.

Proceed with reload of module? [confirm]
% reset issued for module 9
Router#
00:31:11:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:31:11:SP:The PC in slot 9 is shutting down. Please wait ...
00:31:25:SP:PC shutdown completed for module 9
```

```
00:31:25:%C6KPWR-SP-4-DISABLED:power to module in slot 9 set off (admin
request)
00:31:28:SP:Resetting module 9 ...
00:31:28:%C6KPWR-SP-4-ENABLED:power to module in slot 9 set on
00:33:26:%SNMP-5-MODULETRAP:Module 9 [Up] Trap
00:33:26:%DIAG-SP-6-BYPASS:Module 9:Online Diagnostics is Bypassed
00:33:26:%OIR-SP-6-INSCARD:Card inserted in slot 9, interfaces are now
online
Router#

Router# session slot 9 proc 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.91 ... Open

Persistent Storage Module (WS-SVC-PSD-1)

login:root
Password:

Cisco Persistent Storage Module (WS-SVC-PSD-1) Console, 2.2(0.1)
Copyright (c) 1999-2002 by cisco Systems, Inc.

WARNING! Default password has not been changed!
root@localhost.cisco.com#

root@localhost.cisco.com# upgrade ftp://host/pub/rmon/mp.1-1-0-1.bin.gz
user password:

Downloading image...
ftp://host/pub/rmon/mp.1-1-0-1.bin.gz (11065K)
-                         [########################]   11065K |  837.65K/s
11331153 bytes transferred in 13.21 sec (837.64k/sec)

Uncompressing the image...

Verifying the image...

Applying the Maintenance image.
This may take several minutes...

Upgrade of Maintenance image completed successfully.
root@hostname.cisco.com# exit

Router# hardware_module module 9 reset cf:1
Device BOOT variable for reset = cf:1
Warning:Device list is not verified.

Proceed with reload of module? [confirm]
% reset issued for module 9
Router#
02:27:19:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
02:27:19:SP:The PC in slot 9 is shutting down. Please wait ...
02:27:36:SP:PC shutdown completed for module 9
02:27:36:%C6KPWR-SP-4-DISABLED:power to module in slot 9 set off (admin
request)
02:27:39:SP:Resetting module 9 ...
02:27:39:%C6KPWR-SP-4-ENABLED:power to module in slot 9 set on
02:29:37:%SNMP-5-MODULETRAP:Module 9 [Up] Trap
02:29:37:%DIAG-SP-6-BYPASS:Module 9:Online Diagnostics is Bypassed
02:29:37:%OIR-SP-6-INSCARD:Card inserted in slot 9, interfaces are now
online
Router#
```

Upgrading the PSD Application Software

To upgrade the PSD application software, follow these steps:

Step 1 Copy the PSD application software image to a directory accessible to FTP.

Step 2 Log in to the switch through the console port or through a Telnet session.

Step 3 If the PSD is running in the maintenance image, go to Step 4. If the PSD is not running in the maintenance image, enter this command in privileged mode:

```
Router# hardware_module module 9 reset cf:1
Device BOOT variable for reset = cf:1
Warning:Device list is not verified.

Proceed with reload of module? [confirm]
% reset issued for module 9
Router#
00:03:31:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:03:31:SP:The PC in slot 9 is shutting down. Please wait ...
00:03:41:%SNMP-5-COLDSTART:SNMP agent on host R1 is undergoing a cold
start
00:03:46:SP:PC shutdown completed for module 9
00:03:46:%C6KPWR-SP-4-DISABLED:power to module in slot 9 set off (admin
request)
00:03:49:SP:Resetting module 9 ...
00:03:49:%C6KPWR-SP-4-ENABLED:power to module in slot 9 set on
00:05:53:%SNMP-5-MODULETRAP:Module 9 [Up] Trap
00:05:53:%DIAG-SP-6-BYPASS:Module 9:Online Diagnostics is Bypassed
00:05:53:%OIR-SP-6-INSCARD:Card inserted in slot 9, interfaces are now
online
Router#
```

Step 4 After the PSD is back online, establish a console session with the PSD and log in to the root account.

```
Router# session slot 9 proc 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.91 ... Open

Persistent Storage Module (WS-SVC-PSD-1)

Maintenance Partition

login:root
Password:

Persistent Storage Module (WS-SVC-PSD-1) Console, 1.4(1)m
Copyright (c) 1999, 2000, 2001 by cisco Systems, Inc.
```

Step 5 Upgrade the PSD application software by entering:

```
root@localhost# upgrade ftp-url
```

ftp-url is the FTP location and name of the PSD software image file.

Note If the FTP server does not allow anonymous users, use the following syntax for the *ftp-url* value: ftp://user@host/absolute-path/filename. Enter your password when prompted.

Step 6 Follow the screen prompts during the upgrade.

Step 7 After completing the upgrade, log out of the PSD.

Step 8 Reset the PSD to the AP image by entering:

```
Router# hardware_module mod 8 reset
Device BOOT variable for reset =
Warning:Device list is not verified.

Proceed with reload of module? [confirm]
% reset issued for module 8

Router#
00:26:55:%SNMP-5-MODULETRAP:Module 8 [Down] Trap
00:26:55:SP:The PC in slot 8 is shutting down. Please wait ...
```

Step 9 (Optional) Verify the initial configuration after the PSD comes back online by logging into the PSD root account and then entering:

```
root@localhost# show ip
root@localhost# show snmp
```

This example shows how to upgrade the PSD application software:

```
Router# hardware_module module 9 reset cf:1
Device BOOT variable for reset = cf:1
Warning:Device list is not verified.

Proceed with reload of module? [confirm]
% reset issued for module 9

Router#
00:16:06:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:16:06:SP:The PC in slot 9 is shutting down. Please wait ...
00:16:21:SP:PC shutdown completed for module 9
00:16:21:%C6KPWR-SP-4-DISABLED:power to module in slot 9 set off (admin
request)
00:16:24:SP:Resetting module 9 ...
00:16:24:%C6KPWR-SP-4-ENABLED:power to module in slot 9 set on
00:18:21:%SNMP-5-MODULETRAP:Module 9 [Up] Trap
00:18:21:%DIAG-SP-6-BYPASS:Module 9:Online Diagnostics is Bypassed
00:18:21:%OIR-SP-6-INSCARD:Card inserted in slot 9, interfaces are now
online

Router# session slot 9 proc 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.91 ... Open

Persistent Storage Module (WS-SVC-PSD-1)

Maintenance image

login:root
Password:

Maintenance image version:1.4(1)m

root@localhost.cisco.com# upgrade ftp://psdlab-pc1/pub/rmon/c6psd2.2-2-0-8.bin.gz

Downloading the image. This may take several minutes...
ftp://psdlab-pc1/pub/rmon/c6psd2.2-2-0-8.bin.gz (59198K)
/tmp/upgrade.gz           [########################]   59198K |  821.24K/s
```

```
60619473 bytes transferred in 72.08 sec (821.23k/sec)

Upgrade file ftp://psdlab-pc1/pub/rmon/c6psd2.2-2-0-8.bin.gz is downloaded.
Upgrading will wipe out the contents on the hard disk.
Do you want to proceed installing it [y|N]:y

Proceeding with upgrade. Please do not interrupt.
If the upgrade is interrupted or fails, boot into
Maintenance image again and restart upgrade.

Creating PSD application image file...

Initializing the application image partition...
Applying the image, this may take several minutes...
Performing post install, please wait...
Upgrade complete. You can boot from the Application image.

root@hostname.cisco.com# exit

[Connection to 127.0.0.91 closed by foreign host]
Router#

Router# hardware_module module 9 reset
Device BOOT variable for reset =
Warning:Device list is not verified.

Proceed with reload of module? [confirm] y
% reset issued for module 9


Router#
00:24:04:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:24:04:SP:The PC in slot 9 is shutting down. Please wait ...
00:24:18:SP:PC shutdown completed for module 9
00:24:18:%C6KPWR-SP-4-DISABLED:power to module in slot 9 set off (admin
request)
00:24:21:SP:Resetting module 9 ...
00:24:21:%C6KPWR-SP-4-ENABLED:power to module in slot 9 set on
00:26:19:%SNMP-5-MODULETRAP:Module 9 [Up] Trap
00:26:19:%DIAG-SP-6-BYPASS:Module 9:Online Diagnostics is Bypassed
00:26:19:%OIR-SP-6-INSCARD:Card inserted in slot 9, interfaces are now
online
```

Saving and Restoring Configurations

For general information about saving and restoring configurations, refer to the *Catalyst 6000 Family IOS Software Configuration Guide* or to the *Cisco 7600 Series Internet Router IOS Software Configuration Guide*.

The PSD provides a method to save and restore your configuration.

Additionally, if you need to change PSD modules in the Catalyst chassis, you will need to configure the new module. Cisco recommends that you perform the following procedure to save and store your PSD configuration details:

Step 1 Session into the PSD:

```
router# session slot slot_num processor processor
```

Issue the root@localhost.localdomain# **show ip command** and archive the IP address information for future reference.

Step 2 Establish connectivity to an IP server on which to write files.

Step 3 Issue the **configuration save** command.

Note Using certain special characters in a password can cause problems when you issue the **configuration save** command. The characters are as follows: **` & ( ) | ; " ' < >**

If you choose not to put an FTP server on your network, you can use the following instructions to save and restore your configuration.

Step 1 Session into the PSD:

```
    router# session slot slot_num processor processor
```

Step 2 From there, issue the following **show** commands, and copy and paste the various **show** output into your preferred text editor:

```
root@localhost.localdomain# show ip
root@localhost.localdomain# show snmp-agent
root@localhost.localdomain# show datastore all
```

Step 3 Save this file in a secure location for backup purposes.

Restoring

If you need to restore a previous configuration, use the following instructions:

Step 1 Session into the PSD:

```
    router# session slot slot_num processor processor
```

Step 2 Enter the **restore** command. The PSD will reboot 2 or 3 times, will copy the new configuration at boot up and restore the configuration

Step 3 Boot the PSD again, and it reads the command.

Note Issuing the **configuration clear** command clears the configuration, and causes the PSD to go offline. The PSD is still running and ready to be configured with new values. Use this command sparingly.

Note If you restore a configuration that is identical to the existing configuration, the new configuration will overwrite the existing configuration, and the PSD will go through the normal reboot sequence it would use if the configuration had been different.

Other Configuration Tasks

Configuring the Boot Partitions on the PC Image

The PC compact flash is divided into 2 distinct operating systems. There is a Maintenance Partition (MP) that is common to all similar Cisco service cards, and there is an Application Partition (AP) that stores the PSD image. To configure the the MP and AP for the PSD, perform the following commands in global configuration mode:

Command	Purpose

`Router (config)#` **`boot device module`** *`3`* **`hdd:1`**
`Device BOOT variable = cf:1`
`Warning: Device list is not verified.`
	Configures the Application Partition. hdd:1 is the default AP, and cf:1 is the MP.

Note Upon intial power-on the PSD card boots to the application image.

Enter the following router configuration command, where x is the slot number for the PSD:

```
Router(config)# boot device module x hdd:1
```

Note We advise that you only use this procedure when directed by Cisco TAC.

Additional PSD Software Commands

The PSD also supports these CLI commands, which are described in more detail in the *Catalyst 6000 Family IOS Command Reference* publication. These commands are grouped according to mode. These sections describe the Cisco IOS commands that interact with the PSD:

- User and Privileged EXEC Commands, page 1-39
- Configuration Commands, page 1-40
- The "Command Reference" section on page 1-52 lists the PSD Application Commands

User and Privileged EXEC Commands

The following commands are all performed in User and Privileged EXEC mode:

Table 1-8 User and Privileged EXEC Commands

Command	Description

hardware-module module *module_number* **reset** *word*	Resets the module into the application image by default. The fast option allows you to skip the BIOS memory test for a faster boot
	Note If you do not specify a boot device for this command, the **<empty>** message is displayed. For example:
	`Router#  hardware_module module 3 reset`
	`Device BOOT variable for reset = <empty>`
	`Warning:Device list is not verified.`

hw-module module *module_number* **reset** *word* **mem-test-partial**	The same as above, but an abbreviated BIOS RAM check is performed even if the full check is specified in the config of the MSFC2.
hw-module module *module_number* **memory-test-full**	This configuration command sets the boot option on the specified module to the full BIOS RAM check. The default is the abbreviated check.
hw-module module *module_number* **reset cf:1**	Resets the module into the maintenance image.
hw-module module *module_number* **shutdown**	Resets the module into the maintenance image and shuts down the module.
reload	Reloads the entire switch.
remote login switch	Login to the switch processor. Set the debug level with **debug pc** {severe| major} This results in additional diagnostic output on the MSFC2 console.
session slot *slot_number* **processor 1** **telnet** 127.0.0.module+processor (module 7+processor 1 => 127.0.0.71)	These two commands perform the same operation. Either command will drop you into a telnet session on the Multi-Service Feature Card 2 (MSFC2 loopback interface that gives access to the card hosted CLI for the PSD (or other) card in the slot specified).
show interfaces Gigabit *slot_number/port_number*	Displays status of the interface.
show interfaces switchport *module slot_number*	Displays current switch settings for the interfaces.
show interface trunk *module slot_number*	Displays current trunk settings for the interfaces.

Table 1-8 User and Privileged EXEC Commands (continued)

Command	Description
show module	Displays installed modules, versions, and states. **Note** This command does not show the signature level.
show module psd *module_number* **port** *port_number* [**state** | **traffic**]	Displays module information for a specified PSD.
show running-config	Displays the configuration that is currently running.
show startup-config	Displays the saved configuration.

Configuration Commands

The following commands are all performed in either global configuration mode or the interface configuration mode:

- Global Configuration Mode, page 1-40
- Interface Configuration Mode, page 1-40

Global Configuration Mode

The following commands are all performed in global configuration mode:

Command	Description
power enable module *slot_number*	Turns the power on for the PSD if it is not already on.
no power enable module *slot_number*	Shuts down the PSD and removes power.
clock timezone *zone offset*	Sets the timezone for the switch or PSD.
clock summer-time ***zone*** **recurring**	Sets the switch to use summertime settings.
clock calendar valid	Sets the current calendar time as the switch time on startup.
persistent-store module	Sets the PSD vlan that the PSD uses for network traffic.

Interface Configuration Mode

The following commands are configuration commands performed in interface configuration mode:

Command	Description
switchport	Sets interface as a switchport.
switchport trunk encapsulation dot1q	Sets dot1q as the encapsulation type.
switchport trunk native vlan *vlan*	Sets native VLAN for the trunk port.
switchport trunk allowed vlan *vlans*	Sets allowed VLANs for a trunk.
switchport mode trunk	Sets the interface as a trunk port.
switchport capture	Sets the interface as a capture port.
switchport access vlan *vlan*	Sets the access VLAN for the interface.
switchport mode access	Sets the interface as an access port.

MP Commands

Administrators can boot the MP and session into the CLI. There is a set of interfaces available on the MP to administer and diagnose the PSD. One of the key features of the MP is to provide the ability to install a new AP image. The following table summarizes the MP commands:

Table 1-9 MP Command on the PSD

Command	Description
clear log upgrade	Clears the logs generated as a result of upgrade of AP from MP.
clear ip	Clears all the network parameters of the PSD. This includes the ip address, default gateway, domain name server and the domain name. The shared network info stored in a separate partition will be deleted and marked as deleted. Clearing the parameters ensures that there is no clash in IP addresses when the MP is first booted in the field.
disable-guest	Disable the guest account on the MP.
enable-guest	Enables the guest account on the MP.
ip address **[***ip address***]** **[***subnet***]**	Configures the IP address for the PSD used to access the external network.
ip broadcast [*broadcast-address*]	Sets the broadcast ip address.
ip clear	Clears the IP values only.
ip gateway [*default-gateway*]	Specifies the default gateway for the network.
ip host [*host-name*]	Configures the name of the machine.
logout	Logout of the MP shell.
ip nameserver [*name-server1*] [*name-server2*]	Configures the IP addresses of a Domain Name Server. You can configure a maximum of 2 name servers.
passwd	Changes the password for the current user.
passwd-guest	Changes the password for the guest account
ping *host-name* | *IP address*	Pings a specified host on the network, and verifies that the network parameters are configured correctly.
show images	Displays the images stored in the various application partitions. You can use this information to select the device and partition to upgrade.
show ip	Displays the network parameters of the PSD.
show log upgrade	Displays the logs generated as a result of upgrade of AP from MP.
show tech-support	Displays information from the HDD from the MP. It shows information such as boot log and version files. If the AP will not boot, you could boot the MP and use this command to troubleshoot the boot problem and display AP configuration. This command is specific to the PSD. It gathers available diagnostic information from the HDD daughter card, even if the application partition is not bootable.

Table 1-9 MP Command on the PSD

Command	Description
show version	Displays information such as major version, minor version of the MP, CPU type, number of processors on the PC, compact flash/hard disk size, size of DRAM, and other info available in the SMBIOS structures.
syscli	Displays the “Komodo” diagnostics prompt, and accepts all Komodo+ diagnostics commands listed below. This command has no effect and reports no errors when invoked by the root user. It invokes the diagnostic command interpreter when used by the guest account. ⚠ **Caution** The diagnostics available under **syscli** are only meant to be used by TAC. These diagnostic commands are not meant to be part of normal customer operations. • **help** • **ecount** [n] • **edown** *port number* • **elpbk** *port number* • **eping** *port number* • **estat** • **etest** • **komodo+** *options* • **ra** *-d deviceType -n deviceNumber -a action -o offset -v setValues* • **scplog** [*-s* | *-v logLevel*]
upgrade-bios	Upgrades the BIOS on the PSD card.
upgrade *ftp-url* [**--install**] | [**device**:*partition-number*]	Upgrades the image where *ftp-url* is the URL specifying the ftp server containing the image and the path to the image. It will be of the form: ftp://user:password@server-name/path. The name of the ftp server or its IP address can be specified. **Note** If the password is not specified, the user will be prompted to enter the password “--install”

Troubleshooting the PSD

This section provides troubleshooting information for the PSD.

Symptom When a **reset** command is entered from the Supervisor CLI, the system always boots into the maintenance image.

Possible Cause If the boot device is configured in the Supervisor as cf:1, typing a **reset** *module* command always boots to the maintenance image.

Recommended Action Override the configured boot device in the Supervisor by entering the boot string during reset.

- In Cisco IOS software, reconfigure using the **no boot device cf:1** command.

Symptom You are unable to log into the maintenance image with the same password for the PSD application image.

Possible Cause The PSD application image and the maintenance image have different password databases for the root and guest accounts. The default passwords for root and guest differ between the maintenance image and the PSD application image. Any password change performed in the PSD application image does not change the maintenance image password, and vice versa.

Recommended Action Use the maintenance image password.

Symptom You lost your password for the maintenance image and want to recover it.

Possible Cause The maintenance image does not support resetting passwords from the switch. Upgrading the maintenance image sets the password for root and guest to default in the maintenance image.

Recommended Action Use the default maintenance image passwords. Refer to Table 1-6 on page 1-28.

Symptom When the PSD initially boots, by default it runs a partial memory test and you want to run a complete memory test.

Possible Cause The partial memory test is the default configuration.

Recommended Action To perform a full memory test, enter the **hw-module module** *module_number* **reset** *device:partition* **mem-test-full** command.

Note A full memory test takes significantly more time to complete.

You can also use the **hw-module module** *module_number* **memory test full** command. For example:

```
Router# config term
Router(config)#  hw-module module 5 memory test full
Warning:Device list is not verified but still set in the boot string.
```

```
Console> (enable) show boot device module 5
Device BOOT variable = cf:1
Memory-test set to FULL
```

This example shows how to reset the partial memory test:

```
Console> (enable) set boot device cf:1 5
Device BOOT variable = cf:1
Memory-test set to PARTIAL
Warning:Device list is not verified but still set in the boot string.
Console> (enable)
Console> (enable) show boot device module 4
Device BOOT variable = cf:1
Memory-test set to PARTIAL
```

Symptom You cannot connect to the PSD.

Possible Cause The initial configuration is incorrect or not configured.

Recommended Action Reconfigure the PSD as described in the "Configuring the PSD" section on page 1-22.

Symptom The PSD fails to upgrade.

Possible Cause The URL to the server or the image name is incorrect.

Recommended Action Make sure the URL you specified is valid. Make sure the image name you specified in the URL is an official Cisco image name.

Symptom The PSD fails to reconfigure.

Possible Cause The PSD might have experienced a hardware failure.

Recommended Action Refer to the configuration settings that you previously saved.

Symptom You have a corrupt data file, need to check for corrupt data files, or need to identify unread files.

Possible Cause The PSD reloaded, or was improperly shut down.

Recommended Action To check for previously read files that are corrupt, FTP to the PSD and check the "Salvage" directory. Additionally, to identify if any unread files are corrupt, issue the **datastore validate** command.

Note If a datastore is full, issuing this command can take in excess of 30 minutes to complete.

Note You can retrieve data at any time, but you should not destroy a database until the client has read all data.

Standards Compliance Specifications

Refer to Appendix A, “Specifications,” in the *Catalyst 6000 Family Installation Guide* and the *Catalyst 6000 Regulatory Compliance and Safety Information* publication for the standards compliance specifications.

FCC Class B Compliance

This equipment has complies with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco’s installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. There is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco’s written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

Note Modifications to this device not specifically approved by Cisco Systems could void the user’s authority to continue operating the device.

Refer to the *Catalyst 6000 Family Installation Guide* and the *Catalyst 6000 Regulatory Compliance and Safety Information* publication for additional FCC class compliance information.

Copyright Notices

Third-party software used under license accompanies the Cisco Persistent Storage Module Software, release 1.1(1). One or more of the following notices may apply in connection with the license and use of such third-party software.

GNU General Public License

The Persistent Storage Device contains software covered under the GNU Public License. If you would like to obtain the source for the modified GPL code in the Persistent Storage Device, please send a request to psd-sw-req@Cisco.com.

GNU General Public License

License Text

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author’s protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors’ reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The “Program,” below, refers to any such program or work, and a “work based on the Program” means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification”.) Each licensee is addressed as “you.”

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program’s source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

> a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
>
> b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
>
> c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 aboveprovided that you also do one of the following:

> a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a mediumcustomarily used for software interchange; or,
>
> b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing sourcedistribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
>
> c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable.

However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version,” you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. END OF TERMS AND CONDITIONS.

Berkeley Software Distribution License

Various Modules Copyright (C) 1983-2000, The Regents of the Univerisity of California. All rights reserved.

BSD License

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University of California, nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Apache License

Apache

==

The Apache Software License, Version 1.1

Copyright (c) 2000 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: “This product includes software developed by the Apache Software Foundation (http://www.apache.org/).”

   Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The names “Apache” and “Apache Software Foundation” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.
5. Products derived from this software may not be called “Apache”, nor may “Apache” appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see http://www.apache.org/.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.

Related Documentation

- For additional FCC class compliance information, refer to the *Catalyst 6000 Regulatory Compliance and Safety Information* publication.
- For additional infomation about the Cisco Content Services Gateway, refer to the following publications:
  - *Cisco Content Services Gateway Installation and Configuration Guide, Release 3.1(0)C4(x)*
  - *Release Notes for Cisco Content Services Gateway 3.1(1)C4(x)*
- For additional information about Catalyst 6000 family switches and command-line interface (CLI) commands, refer to the following:
  - *Catalyst 6000 Family Software Configuration Guide*
  - *Catalyst 6000 Family Command Reference*
  - *Site Preparation and Safety Guide*
- For detailed hardware configuration and maintenance procedures, refer to the *Catalyst 6000 Family Module Installation Guide*.

Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications. PSD-specific commands are identified.

configuration

To clear all IP and data store configurations, save a PSD configuration to a specified URL, or retrieve a previously saved configuration from a specified URL, use the PSD **configuration** command.

configuration [**clear** | **save** | **restore**] *ftp-url*

Syntax Description

clear *ftp-url*	Clears all IP and data store configurations. This deletes all existing data stores (their associated configuration entries, access list entries, directories and data), and causes the application to restart.
save *ftp-url*	Saves the PSD configuration to a specified URL in the following form: `ftp://username:password@hostname/fully-qualified-destination-directory` The *password* is an optional parameter. If the *password* is not specified in the URL, the user will be prompted for the password. The configuration is archived into a file named **psd.config.***host.date.time*, and placed into the remote relative directory for subsequent retrieval. *host* is the hostname of the PSD. The configuration save includes the version of the PSD from which the configuration was archived for later use.
restore *ftp-url*	Retrieves a previously saved configuration from a specified URL in the following form: `ftp://username:password@hostname/fully-qualified-destination-directory/configuraiton-file-name` • The *password* is an optional parameter. If the *password* is not specified in the URL the user will be prompted for the password. • Restoring a configuration from a newer PSD version to an older PSD version is not permitted, and results in an error message. • The **configuration restore** command notifies you that you have to reboot after you successfully download and apply the configuration. You may choose to cancel. • While the *save* operation generates the target file name, you must fully qualify which one you want to restore. This qualifier allows you to save multiple configuration files, and to select which one to restore. Additionally, you may decide to archive the saved configurations using a custom naming convention. After reboot, the application component will handle the fact that data stores in the restored configuration file may not match with those existing in /cdr-backup directory. If this occurs, a data store entry will be added to the configuration file for each existing data store directory that does not have a corresponding configuration entry. Likewise, a new directory will be created for each data store configuration entry that does not have an associated set of directories.

Defaults

There are no default values for this command.

Command Modes

This is a PSD application-specific command.

Command History

Release	Modification
2.0	This command was introduced.

Usage Guidelines

Using certain special characters in a password can cause problems when you issue the **configuration save** command. The characters are as follows:
` & ( ) | ; " ' < >

Using these characters in a password can cause the following error responses:

response a:

```
Password for psdtest@bizarre.cisco.com:
sh: -c: line 1: unexpected EOF while looking for matching ``'
sh: -c: line 2: syntax error: unexpected end of file
root@inga.cisco.com#
```

response b:

```
Password for psdtest@bizarre.cisco.com:
sh: psd.config.inga.20050322.125632: command not found
root@inga.cisco.com#
    Usage: FTP {store | retrieve} {ascii | binary } <host>
               <username> <password> <local-file> <remote-file>
               [verbose]

           Where:
             <host>       : host name or IP address
             <username>   : user's login id
             <password>   : user's password
             <local-file> : local file name
             <remote-file>: remote file name
root@inga.cisco.com#
```

response c:

```
Password for psdtest@bizarre.cisco.com:
sh: -c: line 1: syntax error near unexpected token `('
sh: -c: line 1: `/opt/psd/bin/ftp.sh store binary bizarre.cisco.com psdtest (
psd.config.inga.20050322.125707 /tftpboot/psd.config.inga.20050322.125707'
root@inga.cisco.com#
```

Examples

The following example shows how to restore a datastore named “cisco”:

```
router# configuration restore ftp://username:password@hostname/cisco
```

datastore

To configure and manage datastores on the PSD, use the PSD **datastore** command.

datastore [create *dsname*] [**destroy** *dsname*] **[access enable** *dsname client-ip port-number*] [**access disable** *dsname client-ip port number*] [**validate** *dsname*]

Syntax Description

create *dsname*	Creates the specified datastore.
destroy *dsname*	Destroys the specified datastore; you will be prompted to confirm.
access enable *dsname client-ip port-number*	Allows the client-IP to access the specified datastore. The *port-number* configures an optional port number. This is the port number (on the accessor) where unsolicited requests from the PSD are sent.
access disable *dsname client-ip port-number*	Disallows the client-IP access to the specified datastore. The *port-number* configures an optional port number. This is the port number (on the accessor) where unsolicited requests from the PSD are sent.
validate *dsname*	Validates the named datastore; you will be prompted to confirm.

Defaults

There are no default settings for this command.

Command Modes

This is a PSD application-specific command.

Command History

Release	Modification
1.0(1)	This command was introduced.
2.0	The *port-number* variable was added.

Usage Guidelines

You cannot destroy a datastore until all associated access entries have been disabled.

Note Large datastores can take wait several minutes to validate.

The port number is used to send unsolicited GTP' Node Alive requests to accessors. The port number may vary from one data store to another. If the port number is not specified no unsolicited messages will be sent from the PSD to the associated accessor.

Examples

The following example shows how to create a datastore named “cisco”, as well as configuring the access list for that datastore:

```
router# datastore create cisco
router# datastore access enable cisco 1.2.3.4 6
router# datastore validate cisco
```

datastore purge transferred

To purge data and/or salvage files that were previously transferred to an FTP server, use the datastore purge transfer PSD application command.

datastore purge transferred {**data-files** | **salvage-files** | **all**} *data-store-name*

Syntax Description

data-files	Purges the specified data files in a specified datastore.
salvage-files	Purges the specified salvage files in a specified datastore.
all	Purges the all files in a specified datastore.
data-store-name	The name of a specified datastore.

Defaults

There are no default settings for this command.

Command Modes

This is a PSD application-specific command.

Command History

Release	Modification
2.0	This command was introduced.

Usage Guidelines

Examples

The following example shows how to purge data files from a datastore named “cisco”.

```
router# datastore purge transferred data-files cisco
```

datastore transfer

To transfer and delete or keep specified files (data-files, salvage-files, or all) of the named datastore from the PSD to a specified URL, use the **datastore transfer** PSD application command.

datastore transfer {**keep** | **delete**} {**data-files** | **salvage-files** | **all**} *data-store-name ftp-url*

Syntax Description

keep	Transfers and keeps the specified files from a specified datastore.
delete	Transfers and deletes the specified files from a specified datastore.
data-files	The specified data files in a specified datastore.
salvage-files	The specified salvage files in a specified datastore.
all	All files in a specified datastore.
data-store-name	The name of a specified datastore.
ftp-url	The specified URL to transfer files to. The format is ftp://*username*:*password@hostname*/*fully-qualified-destination-directory*

Defaults

There are no default settings for this command.

Command Modes

This is a PSD application-specific command.

Command History

Release	Modification
2.0	This command was introduced.

Usage Guidelines

The *password* parameter is optional. If you do not specify the password in the URL, you will be prompted for the password. The password prompt was created to avoid security concerns over being able to look through the command history and seeing a previous “datastore transfer” request with an included password.

If the **delete** option is enabled, the specified files will be transferred to the specified URL, and then deleted. If the **keep** option is specified, the files will be transferred but will not be deleted. You need to issue the **datastore purge** command to delete the transferred files.

Note The **datastore transfer** command can take a long period of time to complete for large data stores; therefore, you can cancel the command using **Ctrl-C**.

Examples

The following example shows how to purge data files from a datastore named “cisco”.

```
router# datastore
```

debug persistent-store

To enable diagnostic information that is dumped to the console to be displayed, use the **debug psd** command in privileged EXEC mode.

debug persistent-store [all | info | error]

Syntax Description

all	Displays all diagnostic information
info	Displays messages that show a trace of the events that are occurring, and in what order they occur.
error	Displays all error information.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
1.0(1)	This command was introduced.

Examples

The following example illustrates how to enable debugging using the **debug persistent-store** command:

```
ce-cat6k-4#debug persistent-store?
  all    all persistent-store debug flags
  debug  debug persistent-store info
  error  debug persistent-store error
  info   debug persistent-store info

ce-cat6k-4#debug persistent-store debug
persistent-store debug debugging is on
```

exit

To log out of system, use the PSD **exit** command.

exit

Syntax Description

No arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
1.0(1)	This command was introduced.

Examples

The following example illustrates the PSD **exit** command:

```
root@localhost# exit
```

ftp-server

To enable ftp access to the datastore repository, use the PSD **ftp-server enable** command. Use the **ftp-server disable** command to disable this function.

ftp-server enable

ftp-server disable

Syntax Description

enable	Enables the FTP server for access to the datastore repository.
disable	Disables the FTP server.

Defaults

The default setting is that the ftp-server is **disabled**.

Command Modes

This is a PSD application-specific command.

Command History

Release	Modification
1.0(1)	This command was introduced.

Usage Guidelines

You must FTP to the PSD device, and login using the root userid and password. You will be placed in the “datastore” directory where you have read access to any files which comprise the datastore(s).

Examples

The following example illustrates how to enable the **ftp-server**:

```
root@localhost# ftp-server
disable                   - disable ftp access for this device
enable                    - enable ftp access for this device
root@localhost# ftp-server enable
```

in-service

To enable the PSD for use by one or more clients, use the PSD **in-service** command in PSD configuration mode.

in-service

Syntax Description

No arguments or keywords.

Defaults

No default behavior or values.

Command Modes

This is a PSD application-specific command.

Command History

Release	Modification
1.0(1)	This command was introduced.

Usage Guidelines

You must issue this command before you send any data to the PSD.

Examples

The following example illustrates the PSD **in-service** command:

```
root@localhost# in-service
```

Related Commands

Command	Description
out-of-service	Prohibits the PSD from receiving any data from one or more clients.

ip

To set various IP parameters on the PSD, use the PSD **ip** command.

ip [address | broadcast | domain | gateway | host | hosts | nameserver]

Syntax Description

address	Sets the system's IP address and subnet.
broadcast	Sets the system's broadcast address.
domain	Sets the system's domain name.
gateway	Sets the system's default gateway-address.
host	Sets the system's host name.
hosts	Adds, deletes, or replaces the hosts entries.
nameserver	Sets the system's nameserver entries.

Defaults

There are no default settings for this command.

Command Modes

This is a PSD application-specific command.

Command History

Release	Modification
1.0(1)	This command was introduced.

Examples

The following example illustrates the **ip hosts add** command:

```
root@localhost# ip hosts add
ip hosts add ip_address host_name [alias1] [alias2]
  or
ip hosts add ftp://user:passwd@host/full-path/filename
```

log

To set various logging parameters on the PSD, use the PSD **log** command.

log [remote enable *ip-addr* | *hostname***] [remote disable] [supervisor enable] [supervisor disable] [category enable** *category level* | **category disable** *category level***] [default** *level***]**

Syntax Description

remote enable	Enables remote logging and forwards any messages to the remote host. Only one host may be specified.
ip-addr	Sets the IP address of the host.
hostname	Sets the host name.
remote disable	Disables the remote logging.
supervisor enable	Enables messages to be logged to the Supervisor. Syslog messages of type "critical," "alert," or "fatal" are candidates for IOS logging.
supervisor disable	Disables supervisor logging of messages.
category enable *category level*	Enables the logging level for the specified logging category. Category granular logging is intended to be used at the direction of TAC as the output messages are used to pinpoint errors You can view the list of categories by using the **log category enable ?**, or **show log-settings** commands. Category level may be one of the following: • Fatal • Error • Warning • Info • Debug • Trace

category disable *category*	Resets logging for the speicified category to the default level. The Category level may be one of the following: • Fatal • Error • Warning • Info • Debug • Trace
default *level*	Sets the default logging level for the platform. By setting a category at a finer logging level, it is possible to debug/monitor individual categories. Level may be one of the following: • Fatal • Error • Warning • Info • Debug • Trace

Defaults

The default logging level is “info”.

Command Modes

This is a PSD application-specific command.

Command History

Release	Modification
1.0(1)	This command was introduced.

Usage Guidelines

Caution Setting the logging level to “debug” or “trace” will adversely affect the PSD’s performance. These levels should only be used by Cisco TAC.

Examples

The following example sets the PSDs **log** level default to **info**:

```
root@localhost# log
category                  - enable or disable category logging and levels
default                   - set system’s default logging level
remote                    - set address to forward system's log messages
supervisor                - enable or disable the supervisor logging
root@localhost# log default
debug                     - Set default logging level to 'debug'
error                     - Set default logging level to 'error'
fatal                     - Set default logging level to 'fatal'
info                      - Set default logging level to 'info'
trace                     - Set default logging level to 'trace'
```

```
warn                      - Set default logging level to 'warn'
root@locqlhost# log default info
root@localhost#
```

logout

To log out of system, use the PSD **logout** command.

logout

Syntax Description

There are no keywords or arguments for this command.

Defaults

There are no default settings for this command.

Command Modes

This is a PSD application-specific command.

Command History

Release	Modification
1.0(1)	This command was introduced.

Examples

The following example illustrates the logout command:

```
root@localhost# logout
```

nslookup

To query nameservers, use the PSD **nslookup** command.

nslookup [**hostname** | **ip-address**]

Syntax Description

hostname	Sets the hostname of the nameserver. Only one host may be specified.
ip-address	Sets the IP address of the host.

Defaults

There are no default settings for this command.

Command Modes

This is a PSD application-specific command.

Command History

Release	Modification
1.0(1)	This command was introduced.

Examples

The following example illustrates the PSD **nslookup** command:

```
root@localhost# nslookup
nslookup hostname [server]
```

out-of-service

To prohibit the PSD from receiving any data from one or more clients, use the PSD **out of service** command.

out-of-service

Syntax Description

No arguments or keywords.

Defaults

The PSD boots in an “out-of-service” state. You must put the PSD inservice to store data.

Command Modes

This is a PSD application-specific command.

Command History

Release	Modification
1.0(1)	This command was introduced.

Usage Guidelines

This setting remains in effect until an administrator issues the **in-service** command.

Examples

The following example illustrates the PSD **out-of-service** command:

```
root@localhost# out-of-service
```

Related Commands

Command	Description
in-service	Enables the PSD for use by one or more clients.

password clear

To clear all previous passwords for the root user, use the PSD **password clear** command.

password clear

Syntax Description

There are no keywords or arguments for this command.

Defaults

Issuing this command returns the PSD to the default password settings.

Command Modes

This is a PSD application-specific command.

Command History

Release	Modification
1.0(1)	This command was introduced.

Examples

The following example illustrates the PSD **password clear**command:

```
root@localhost# password clear
```

password root

To set a new password for the root user, use the PSD **password** command.

password root

Syntax Description

There are no keywords or arguments for this command.

Defaults

There are no default settings for this command.

Command Modes

This is a PSD application-specific command.

Command History

Release	Modification
1.0(1)	This command was introduced.

Examples

The following example illustrates the PSD **password** command:

```
root@localhost# password root
Changing password for user root.
New UNIX password: password
Retype new UNIX password: password
passwd: all authentication tokens updated successfully
```

Note If you receive a message “BAD PASSWORD: it is too short,” you can ignore it, as it is only informational.

persistent-store module

To configure a vlan for the PSD module to use for network traffic, use the PSD **persistent-store module** command. To unconfigure this vlan setting, use the **no** form of the command.

persistent-store module *slot* **vlan** *vlan_id*

no persistent-store module *slot* **vlan** *vlan_id*

Syntax Description

slot	Identifies the slot number where the persistent storeage module resides.
vlan *vlan_id*	Sets the identity of the vlan that the PSD uses for network traffic.

Defaults

The default setting is vlan1.

Command Modes

Global configuration.

Command History

Release	Modification
1.0(1)	This command was introduced.

Examples

The following example illustrates the PSD **persistent-store module** command:

```
router# persistent-store module 4 vlan 100
```

ping

To ping a network device, use the PSD **ping** command.

ping [**-nv** | **-c count** | **-i wait** | **-w deadline** | **-p pattern** | **-s packetsize**] {**hostname | IP address**}

Syntax Description

-n	Show network addresses as numbers.
-v	Verbose output.
-c count	Stop after sending count ECHO_REQUEST packets.
-i wait	The amount wait seconds between sending each packet.
-w deadline	The time for ping to wait.
-p pattern	Up to 16 pad bytes to fill out packets sent.
-s packetsize	The 8 bytes of ICMP header data.
hostname	The host name of the pinged device.
ip address	The IP address of the host.

Defaults

There are no default settings for this command.

Command Modes

This is a PSD application-specific command.

Command History

Release	Modification
1.0(1)	This command was introduced.

Usage Guidelines

Configuring **ping** on the PSD to an IP address in the same subnet as the PSD, if the host is unreachable the console returns a "Destination Host Unreachable" message, and the PSD attempts to ping a non-responsive IP address.

```
ping non-responsive-ip-address
```

The **ping** command executes, and output appears; however, the **ping** command never completes, and does not return control to the user.

To recover from the problem, use **ctrl-c** to abort the **ping** command.

Additionally, to avoid the problem, use the **-w deadline** option, and a reasonable timeout to force the command to timeout.

```
ping -w deadline 5 ip-address
```

Generally, the "5" represents the number of seconds before **ping** will exit. Use a larger number if needed.

Examples

The following example illutrates the PSD **ping pattern** command:

```
root@localhost# ping p
root@gretel.cisco.com# ping p
```

```
PING p.cisco.com (10.83.133.67) from 172.18.12.217 : 56(84) bytes of data.
64 bytes from p.cisco.com (10.83.133.67): icmp_seq=1 ttl=57 time=58.3 ms
64 bytes from p.cisco.com (10.83.133.67): icmp_seq=2 ttl=57 time=58.5 ms
64 bytes from p.cisco.com (10.83.133.67): icmp_seq=3 ttl=57 time=57.8 ms
64 bytes from p.cisco.com (10.83.133.67): icmp_seq=4 ttl=57 time=59.3 ms
64 bytes from p.cisco.com (10.83.133.67): icmp_seq=5 ttl=57 time=57.7 ms

--- p.cisco.com ping statistics ---
5 packets transmitted, 5 received, 0% loss, time 4039ms
rtt min/avg/max/mdev = 57.767/58.391/59.373/0.572 ms
```

reboot

To reboot the PSD, use the PSD **reboot** command.

reboot

Syntax Description

There are no keywords or arguments for this command.

Defaults

There are no default settings for this command.

Command Modes

This is a PSD application-specific command.

Command History

Release	Modification
1.0(1)	This command was introduced.

Examples

The following example illustrates the PSD **reboot** command:

```
root@localhost# reboot
```

show

To show system parameters, use the PSD **show** command.

show [status] [statistics gtp-prime] [datastore *dsname* | **all**] [**statistics] [log-settings] [log** *number* | *all* **] [bios** | **cpu** | **date** | **hosts** | **ip** | **log-upgrade** | **memory** | **rx-counters] [snmp-agent] [tech-support] [version]**

Syntax Description

status	Summary of the current state of the PSD in fairly brief output, this is where the application will contribute its current status (i.e. this used to be the PSD SHOW STATUS command).
statistics gtp-prime	The **show statistics** command shows low level statistics for the PSD. Currently the only option is to show gtp-prime statistics. These are used to show any gtp' traffic counters mainly intended for Cisco technical assistance, to assist with troubleshooting.
datastore [*dsname* | *all*] [*statistics*]	Shows Persistent Store Application datastores. Either *dsname* or **all** are required, **statistics** is always optional. If a datastore name is given, then that datastore and its access list is shown. If **all** is specified, then show a list of all datastores defined and access controls. If **statistics** is given, then the output is more verbose showing all of the traffic statistics per CSG in the access list. **Note** This option will not tab-complete from the CLI; however, you can shorten the spelling when specified.
log-settings	Shows a list of the logging categories and their current logging levels. Shows the default log level. Shows the state of any IOS or remote host logging.
log *number* | *all*	Shows the PSD log, line by line (without pagination). • If no argument is specified, then the last 100 lines of the log are presented. • If *all* is specified, the entire log is presented line by line to the console. **Caution** Use *all* with caution as the log file can be large. • If *number* is specified, then the last “number” lines of the log are displayed line by line.
bios	Shows BIOS information.
cpu	Shows cpu utilization.
date	Shows current date and time.
hosts	Shows hosts entries.
ip	Shows ip parameters.
log-upgrade	Shows log upgrade parameters.

memory	Shows memory.
rx-counters	Shows rx-counter variables.
snmp-agent	Shows snmp-agent parameters.
tech-support	Typically, **show tech support** should only be used by Cisco TAC: Shows a variety of information at the display; however, shows only 100 of the last lines of logs to cut down on the amount of output. Use the **tech-support** command to gather all information, and to FTP it to a remote location for debugging, or to send it to TAC. The **show tech-support** command is also available from the MP CLI. It will contain info that will help troubleshoot why an AP is not booting.
version	Shows version information.

Defaults

There are no default settings for this command.

Command Modes

This is a PSD application-specific command.

Command History

Release	Modification
1.0(1)	This command was introduced.

Examples

The following example illustrates the PSD **show** command:

```
root@localhost# show status
status: in-service
```

show module persistent-store

To show state information about the specified port of the specified slot, use the **show module psd** command.

show module persistent-store *slot* **port** *1-3* **[state | traffic]**

Syntax Description

state	Displays state information regarding gigabit ethernet interfaces on the PSD.
traffic	Displays traffic information regarding.

Defaults

There are no default settings for this command.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
1.0(1)	This command was introduced.

Usage Guidelines

There are 3 ports open, but the PSD only use port 1 and port 3. IOS does not support “hiding” unused ports, such as port (2).

Examples

The following example illustrates the variables of the **show module persistent-store** command:

```
router#show module persistent-store 4 port 3 traffic
persistent-store module 4, port 3:

  Hardware is C6k 1000Mb 802.3, address is 0008.7ca8.4792 (bia 0008.7ca8.4792)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Last input never, output 1w1d, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     16990 packets input, 25606961 bytes, 0 no buffer
     Received 30 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     9513 packets output, 627237 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
router#
```

```
router#show module persistent-store 4 port 3 state
persistent-store module 4, port 3:
 This port (Gi4/3) is not a switchable interface
cat 6k#
```

show tech-support

To generate show output when the PSD application is not functioning, use the **show tech-support** command in the Application Partition image.

show tech-support

Syntax Description

There are no keywords or arguments for this command.

Defaults

There are no default values for this command.

Command Modes

AP command.

Command History

Release	Modification
1.0(1)	This command was introduced.

Examples

The following example illustrates the variable of the **show tech-support** command

```
root@localhost# show tech-support
```

Related Commands

Command	Description
tech-support	Generates and ftps a tech-support file to a remote host.

shutdown

To start the shutdown procedure on the PSD, use the PSD **shutdown** command .

shutdown

Syntax Description

There are no keywords or arguments for this command.

Defaults

There are no default values for this command.

Command Modes

PSD-specific command.

Command History

Release	Modification
1.0(1)	This command was introduced.

Examples

The following example illustrates how to issue the **shutdown** command:

```
root@localhost# shutdown
```

snmp-agent

To set snmp-agent parameters, use the PSD **snmp-agent** command.

snmp-agent [**community** | **contact** | **delete** | **enable** | **disable** | **location** | **name**

Syntax Description

community	Sets the device community string; there is not a default "read" community string, and no "write" community string is allowed.
contact	Sets the device contact information.
delete	Deletes the device community string.
enable	Enables the snmp agent. The default setting is disabled.
disable	Disables the snmp agent.
location	Sets the device location.
name	Sets the device name.

Defaults

The default setting is that **snmp-agent** is disabled.

Command Modes

This is a PSD application-specific command.

Command History

Release	Modification
1.0(1)	This command was introduced.

Examples

The following example enables the snmp-agent, and sets the community string to "read":

```
root@localhost# snmp-agent
community                 - set device community string
contact                   - set device contact information
delete                    - delete SNMP community string
disable                   - disable snmp for this device
enable                    - enable snmp for this device
location                  - set device location
name                      - set device name
root@localhost# snmp-agent enable
root@localhost# snmp-agent community
snmp-agent community community-string
root@localhost# snmp-agent community read
root@localhost#
```

tech-support

To generate and ftp a tech-support file to remote host, use the PSD **tech-support** command.

tech-support *ftp://user:passwd@host/relative-path/*

Syntax Description

user	The user name on the remote host.
passwd	The “user'” password, will be prompted for if omitted.
host	The remote host to upload the coredump file(s) to.
relative-path	A directory relative to the user’s default directory. **Note** The specific filename will be generated by the tech-support command so you only need to supply a valid directory name to place the file in.

Defaults

The default setting is that the telnet-server is disabled.

Command Modes

This is a PSD application-specific command.

Command History

Release	Modification
1.0(1)	This command was introduced.

Usage Guidelines

This command will only allow telnet logins, and does not support SSH.

Examples

The following example generates and ftps a tech-support file to remote host “ts” (userid “ken” with password “kp”) and place in the users’s incoming directory (the directory must already exist):

```
router# tech-support ftp://ken:kp@ts:/incoming
```

The file name generated is:

psd.hostname.Mar2003.08:32:22AM

Where “hostname” is the host name of the PSD from which you entered the tech-support command. The date and time will be the current date and time the command was issued. This naming convention avoids file name confusion when you issue **tech-support** from a variety of PSDs, or from the same PSD at different times.

Related Commands

Command	Description
show tech-support	Generates show output when the PSD application is not functioning.

telnet-server

To enable outside logins, use the **telnet-server enable** command. Use the **telnet-server disable** command to disable this function.

telnet-server enable

telnet-server disable

Syntax Description

enable	Enables outside logins using telnet.
disable	Disables outside logins using telnet.

Defaults

The default setting is that the telnet-server is **disabled**. When **enabled**, the telnet server will use port 23.

Command Modes

This is a PSD application-specific command.

Command History

Release	Modification
1.0(1)	This command was introduced.

Usage Guidelines

This command will only allow telnet logins, and does not support SSH.

Examples

The following example uses **telnet-server** command to enable the telnet server:

```
root@localhost# telnet-server enable
```

traceroute

To establish a traceroute to a network device, use the **traceroute** command.

traceroute [-Inv] [-f first_ttl] [-m max_ttl] [-p port] [-s src_addr] [-t tos] [-w waittime] [destination host name | IP address [packetlen]

Syntax Description

I	ICMP ECHO instead of UDP datagrams..
n	Print hop addresses numerically.
v	Verbose output.
first_ttl	The initial time-to-live used in the first packet.
max_ttl	The maximum time-to-live (max number of hops) used.
port	The base UDP port number used in probes.
src_addr	Loose source traceroute, other src than this host.
tos	The type-of-service in packets to the following value.
waittime	The time to wait for a response to a probe.
destination hostname	
IP address	
packetlen	

Defaults

There are no default settings for this command.

Command Modes

This is a PSD application-specific command.

Command History

Release	Modification
1.0(1)	This command was introduced.

Examples

The following example illustrates the **traceroute verbose** command:

```
root@localhost# traceroute -v
```

upgrade

To download and install a new AP or MP image, use the PSD **upgrade** command. You must specify an ftp-url, which is the new AP or MP image you want to install.

upgrade *ftp_url* [**--install**]

Syntax Description

ftp_url	*ftp-url* specifys the new MP image you want to install. The *ftp_url* is in the form of “*ftp://userid[:password]@host[:][/]relative_path*”
“ftp://”	Indicates the use of the FTP protocol for the downoload, currently FTP is the only supported protocol.
“userid”	The userid used to log into the remote host.
[:password]	(Optional) Allows you to specify a password on the command line. If not specified, then you will be prompted for the password.
“@”	Required delimiter preceeding the host.
[:]	(optional) Delimiter between the host and path, specify the colon when you do not want to specify a "/". Some ftp servers will interpret the “/” to indicate a system root path so to circumvent this specify a colon and no leading “/” for the specification to be relative.
[relative_path]	The relative specification to the image, relative to the FTP user’s default directory.

Defaults

There are no default values.

Command Modes

EXEC

Command History

Release	Modification
1.0(1)	This command was introduced.

Usage Guidelines

When you boot to the MP, *ftp_url* specifies an Application Image file (AP). The [**--install**] varible only applies to this usage.

When you boot to the AP, *ftp_url* specifies a Maintenance Image file (MP). The [**--install**] varible does not apply to this usage.

Caution Do not cancel the upgrade, remove the module, or power down the module during the upgrade procedure. Doing so may cause the module to fail to come online.

Examples

The following example illustrates the **upgrade** command:

```
root@localhost# upgrade ftp://user:passwd@host/full-path/filename
```