CISCO SYSTEMS

Installation and Setup Guide for the Cisco 1101 VLAN Policy Server

Corporate 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: 408 526-4100

Customer Order Number: DOC-7814482=
Text Part Number: 78-14482-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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: 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. However, 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.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.

- Move the equipment to one side or the other of the television or radio.

- Move the equipment farther away from the television or radio.

- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

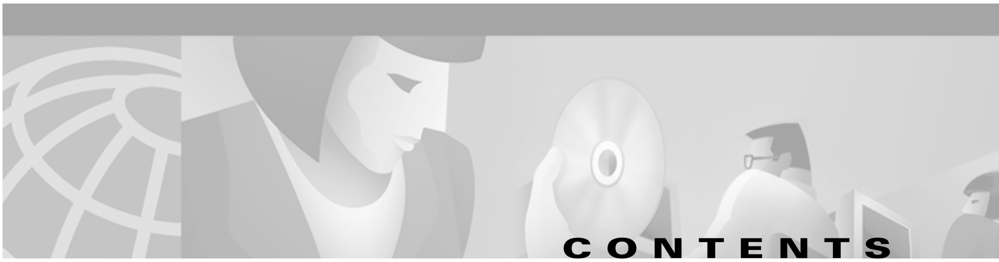
Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

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.

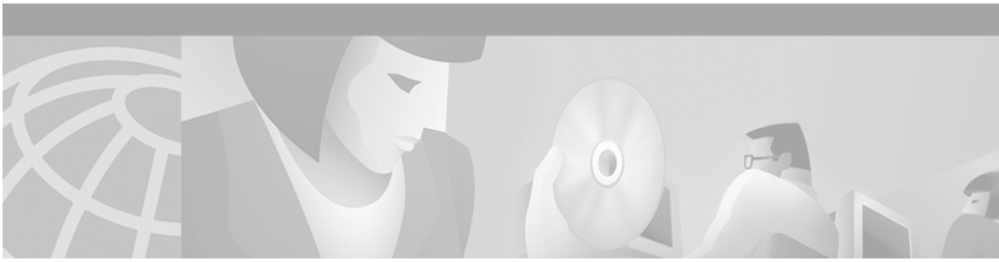
NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Installation and Setup Guide for the Cisco 1101 VLAN Policy Server



CONTENTS



Preface

This guide describes how to install, configure, and administer the VLAN Policy Server.

Audience

This guide is intended primarily for system administrators responsible for installing and configuring internetworking equipment who are familiar with Cisco IOS software.

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

Organization

This guide consists of the following chapters and appendixes:

- Preface
- Product Overview
- Preparing for Installation
- Installing and Configuring the VLAN Policy Server
- Administering the VLAN Policy Server
- Troubleshooting
- Technical Specifications
- Command Reference

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	**boldface** font
Variables for which you supply values	*italic* font
Displayed session and system information	`screen` font
Information you enter	**`boldface screen`** font
Variables you enter	*`italic screen`* font
Menu items and button names	**boldface** font
Selecting a menu item	**Option** > **Network Preferences**

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

Caution Means *reader be careful*. You are capable of doing something that might result in equipment damage or loss of data.

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.**

Waarschuwing **Dit 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.**

Varoitus **Tämä 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).**

Attention **Ce 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.**

Warnung **Dieses 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.**

Avvertenza **Questo 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.**

Advarsel **Dette 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 de advarslene 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.**

Aviso **Este 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.**

¡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.**

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 vara medveten 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.**

Related Documentation

The following documentation is also available:

Paper Documentation

- *Release Notes for Cisco Secure User Registration Tool and the Cisco VLAN Policy Server.*
- *Regulatory Compliance and Safety Information for the Cisco 1101 VLAN Policy Server*

Online Documentation

- Context-sensitive online help

  You can access the help in two ways:

  – Select an option from the navigation tree, then click **Help.**

  – Click the Help button in the dialog box.

- PDF documentation—The following documents can be found in PDF form on the User Registration Tool VPS Recovery CD-ROM:

  – *User Guide for the Cisco Secure User Registration Tool*

  – *Installation and Setup Guide for the Cisco Secure User Registration Tool*

  – *Regulatory Compliance and Safety Information for the Cisco 1101 VLAN Policy Server*

  – *User Registration Tool Software Developer's Guide*

  Note Adobe Acrobat Reader 4.0 or later is required.

- Supported device list for URT

  This can be viewed at the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/fam_prod/user_reg/2_5/urt_dvcs.htm

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

http://www.cisco.com

Translated documentation is available at the following URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Feedback** at the top of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com logon ID and password. If you have a valid service contract but do not have a logon ID or password, go to the following URL to register:

http://www.cisco.com/register/

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

CHAPTER 1

Product Overview

The VLAN Policy Server 1101 is a network management device that runs a common set of management services and the User Registration Tool (URT) VLAN Policy Server (VPS).

For detailed information about installing URT on your VPS, see *Installation and Setup Guide for the Cisco Secure User Registration Tool*, including the “Summary of Installation Tasks” section.

For detailed information about URT, see *User Guide for the Cisco Secure User Registration Tool.*

This chapter contains the following sections:

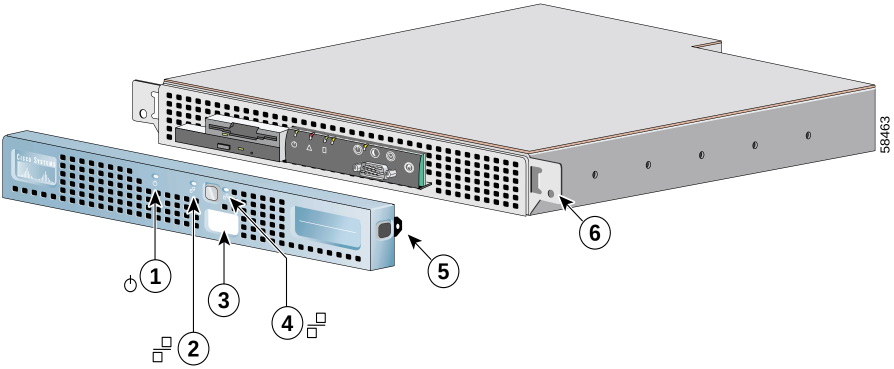
- Bezel Features, page 1-2
- Front Panel Features, page 1-3
- Back Panel Features, page 1-6

Bezel Features

The VLAN Policy Server has a bezel that attaches to its front and covers the front panel. This bezel contains two Ethernet indicators, a power indicator, and a power button, and provides access to the console/serial port. Figure 1-1 shows the bezel's features.

To install the bezel, insert the tabs on each end of the bezel into the flanges on each side of the VLAN Policy Server. To remove the bezel, press the tabs and lift it from the chassis.

Figure 1-1 Bezel Features



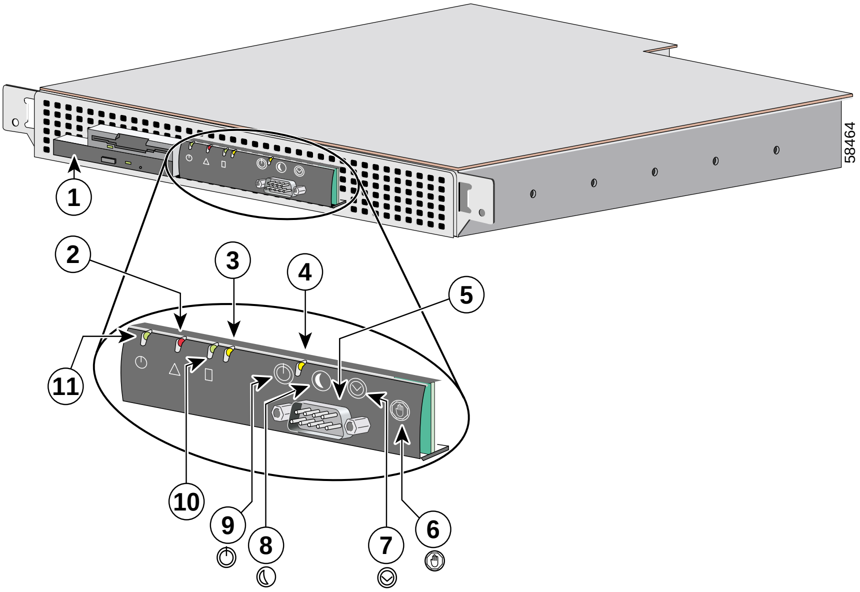
1	Power indicator
2	Ethernet 0 activity/link indicator
3	Console/serial port access
4	Ethernet 1 activity/link indicator
5	Bezel mounting tabs (2)
6	Flanges (2)

Front Panel Features

The VLAN Policy Server front panel contains switches (see System Switches, page 1-5), indicators (see System Indicators, page 1-4), a CD-ROM drive, and the console/serial port. To access the front panel, remove the bezel. Figure 1-2 shows the front panel features.

Note When connecting a console to the VLAN Policy Server, use the console/serial port on the front panel. Do not use the serial port located on the rear panel of the VLAN Policy Server.

Figure 1-2 Front Panel Features



1	CD-ROM drive
2	System fault indicator
3	Ethernet 0 activity/link indicator
4	Ethernet 1 activity/link indicator

5	Console/serial port
6	Non-maskable interrupt switch
7	Reset switch
8	Sleep switch (not supported)
9	Power switch
10	Hard drive indicator
11	Power indicator

System Indicators

When troubleshooting your system, you might need to check the status of the indicators on the system front panel, shown in Figure 1-2. The appearance and function of these lights are described in Table 1-1.

Table 1-1 System Indicators

Indicator	Color	Function
Power	Green	The power indicator lights up when the VLAN Policy Server is connected to an AC power source, and blinks when the VLAN Policy Server is in sleep mode. The bezel contains a duplicate of this indicator.
System fault	Amber	The system fault indicator blinks during system startup and when a system fault is detected. This indicator is not visible with the bezel attached.
Hard drive activity	Green	The hard drive activity indicator blinks when hard drive activity occurs. This indicator is not visible with the bezel attached.

Table 1-1 System Indicators (continued)

Indicator	Color	Function
Ethernet 0 activity/link	Amber	The Ethernet 0 activity/link indicator lights up when the Ethernet 0 port is connected to a network, and blinks when activity occurs on this channel. The bezel contains a duplicate of this indicator.
Ethernet 1 activity/link	Amber	The Ethernet 1 activity/link indicator lights up when the Ethernet 1 port is connected to a network, and blinks when activity occurs on this channel. The bezel contains a duplicate of this indicator.

System Switches

Figure 1-2 shows the location of the switches on the VLAN Policy Server front panel. To activate a switch, press the corresponding icon on the front panel, as shown in Figure 1-2. Table 1-2 describes the function of these switches.

Table 1-2 Front-Panel Switches

Switch	Function
Power switch	The power switch turns the VLAN Policy Server power on or off. To turn system power off, press and hold this switch for at least 4 seconds. There is a power switch on both the bezel and the front panel.
Sleep switch	The sleep switch places the system in sleep mode. This switch is accessible only when the bezel is removed.

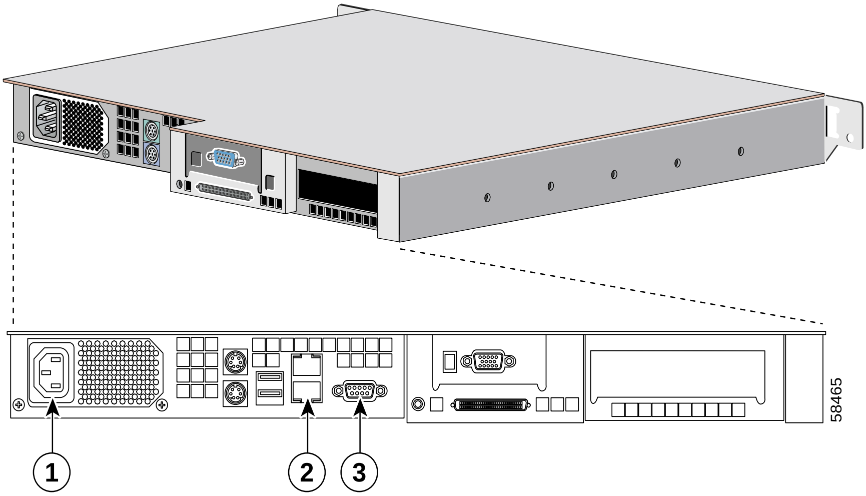
Table 1-2 Front-Panel Switches (continued)

Switch	Function
Reset switch	The reset switch reboots the system. If you cannot shut down the VLAN Policy Server using the operating system, press the reset switch. This switch is accessible only when the bezel is removed.
Non-Maskable Interrupt switch	Use this switch only when instructed to do so by the Cisco Technical Assistance Center (TAC). This switch is accessible only when the bezel is removed.

Back Panel Features

The back panel contains the VLAN Policy Server AC power receptacle, Ethernet connectors, and a serial port. Figure 1-3 shows the back panel connections. Do not attach peripheral devices, such as mice, monitors, and keyboards, to the VLAN Policy Server. It does not support their use.

Figure 1-3 Back Panel Connections



1	AC power receptacle
2	Ethernet connectors (Ethernet 0 is the lower port, and Ethernet 1 is the upper port)
3	Serial port

Serial Ports

The two integrated serial ports, on the front and back panels of the system, use 9-pin D-subminiature connectors.

Serial Port Connectors

If you reconfigure your hardware, you may need pin number and signal information for the serial port connectors. Figure 1-4 shows the pin numbers for the serial port connectors, and Table 1-3 defines the pin assignments and interface signals for the serial port connectors.

Figure 1-4 Pin Numbers for the Serial Port Connectors

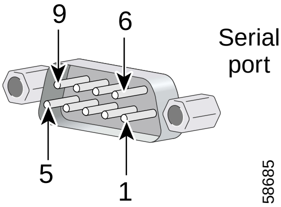


Table 1-3 Serial Port Pin Assignments

Pin	Signal	I/O	Definition
1	DCD	I	Data carrier detect
2	SIN	I	Serial input
3	SOUT	O	Serial output
4	DTR	O	Data terminal ready
5	GND	N/A	Signal ground
6	DSR	I	Data set ready
7	RTS	O	Request to send
8	CTS	I	Clear to send
9	RI	I	Ring indicator
Shell	N/A	N/A	Chassis ground

Ethernet Connectors

Your system has integrated 10/100–Mbps Ethernet connectors. Each Ethernet connector provides all the functions of a network expansion card and supports both the 10BASE-T and 100BASE-TX Ethernet standards.

Warning **To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.**

Waarschuwing **Om elektrische schokken te vermijden, mogen veiligheidscircuits met extra lage spanning (genaamd SELV = Safety Extra-Low Voltage) met telefoonnetwerkspanning (TNV) circuits verbonden worden. LAN (Lokaal netwerk) poorten bevatten SELV circuits en WAN (Regionaal netwerk) poorten bevatten TNV circuits. Sommige LAN en WAN poorten gebruiken allebei RJ-45 connectors. Ga voorzichtig te werk wanneer u kabels verbindt.**

Varoitus **Jotta vältyt sähköiskulta, älä kytke pienjännitteisiä SELV-suojapiirejä puhelinverkkojännitettä (TNV) käyttäviin virtapiireihin. LAN-portit sisältävät SELV-piirejä ja WAN-portit puhelinverkkojännitettä käyttäviä piirejä. Osa sekä LAN- että WAN-porteista käyttää RJ-45-liittimiä. Ole varovainen kytkiessäsi kaapeleita.**

Attention **Pour éviter une électrocution, ne raccordez pas les circuits de sécurité basse tension (Safety Extra-Low Voltage ou SELV) à des circuits de tension de réseau téléphonique (Telephone Network Voltage ou TNV). Les ports du réseau local (LAN) contiennent des circuits SELV et les ports du réseau longue distance (WAN) sont munis de circuits TNV. Certains ports LAN et WAN utilisent des connecteurs RJ-45. Raccordez les câbles en prenant toutes les précautions nécessaires.**

Warnung **Zur Vermeidung von Elektroschock die Sicherheits-Kleinspannungs-Stromkreise (SELV-Kreise) nicht an Fernsprechnetzspannungs-Stromkreise (TNV-Kreise) anschließen. LAN-Ports enthalten SELV-Kreise, und WAN-Ports enthalten TNV-Kreise. Einige LAN- und WAN-Ports verwenden auch RJ-45-Steckverbinder. Vorsicht beim Anschließen von Kabeln.**

Avvertenza **Per evitare scosse elettriche, non collegare circuiti di sicurezza a tensione molto bassa (SELV) ai circuiti a tensione di rete telefonica (TNV). Le porte LAN contengono circuiti SELV e le porte WAN contengono circuiti TNV. Alcune porte LAN e WAN fanno uso di connettori RJ-45. Fare attenzione quando si collegano cavi.**

Advarsel **Unngå å koble lavspenningskretser (SELV) til kretser for telenettspenning (TNV), slik at du unngår elektrisk støt. LAN-utganger inneholder SELV-kretser og WAN-utganger inneholder TNV-kretser. Det finnes både LAN-utganger og WAN-utganger som bruker RJ-45-kontakter. Vær forsiktig når du kobler kabler.**

Aviso **Para evitar choques eléctricos, não conecte os circuitos de segurança de baixa tensão (SELV) aos circuitos de tensão de rede telefónica (TNV). As portas LAN contêm circuitos SELV e as portas WAN contêm circuitos TNV. Algumas portas LAN e WAN usam conectores RJ-45. Tenha o devido cuidado ao conectar os cabos.**

¡Advertencia! **Para evitar la sacudida eléctrica, no conectar circuitos de seguridad de voltaje muy bajo (safety extra-low voltage = SELV) con circuitos de voltaje de red telefónica (telephone network voltage = TNV). Los puertos de redes de área local (local area network = LAN) contienen circuitos SELV, y los puertos de redes de área extendida (wide area network = WAN) contienen circuitos TNV. En algunos casos, tanto los puertos LAN como los WAN usan conectores RJ-45. Proceda con precaución al conectar los cables.**

Varning! **För att undvika elektriska stötar, koppla inte säkerhetskretsar med extra låg spänning (SELV-kretsar) till kretsar med telefonnätspänning (TNV-kretsar). LAN-portar innehåller SELV-kretsar och WAN-portar innehåller TNV-kretsar. Vissa LAN- och WAN-portar är försedda med RJ-45-kontakter. Iaktta försiktighet vid anslutning av kablar.**

Network Cable Requirements

Your VLAN Policy Server Ethernet connectors are designed for attaching an unshielded twisted-pair (UTP) Ethernet cable equipped with standard RJ-45 compatible plugs. Press one end of the UTP cable into the Ethernet connector until the plug snaps securely into place. Connect the other end of the cable to an RJ-45 jack wall plate or to an RJ-45 port on a UTP concentrator or hub, depending on your network configuration. Observe the following cabling restrictions for 10BASE-T and 100BASE-TX networks:

- For 10BASE-T networks, use Category 3 or higher wiring and connectors.
- For 100BASE-TX networks, use Category 5 or higher wiring and connectors.
- The maximum cable run length (from a workstation to a concentrator) is 328 feet or 100 meters.
- For 10BASE-T networks, the maximum number of daisy-chained concentrators on one network segment is four.

Note To avoid line interference, voice and data lines must be in separate sheaths.

CHAPTER 2

Preparing for Installation

This chapter describes the safety instructions and site requirements needed for installing the VLAN Policy Server, and guides you through installation preparation. It contains the following sections:

- Safety, page 2-1
- Preparing Your Site for Installation, page 2-7
- Precautions for Rack Mounting, page 2-10
- Precautions for Products with Telecommunications Options, page 2-11
- Required Tools and Equipment, page 2-11

Safety

This section provides safety information for installing this product.

Warnings and Cautions

Read the installation instructions in this document before you connect the system to its power source. Failure to read and follow these guidelines could lead to an unsuccessful installation and possible damage to the system and components.

You should observe the following safety guidelines when working with any equipment that connects to electrical power or telephone wiring. They can help you avoid injuring yourself and damaging the VLAN Policy Server.

The following warnings and cautions are provided to help you prevent damage to the devices or injury to yourself:

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 **The safety cover is an integral part of the product. Do not operate the unit without the safety cover installed. Operating the unit without the cover in place will invalidate the safety approvals and pose a risk of fire and electrical hazards.**

Warning **Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.**

Warning **Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units.**

Warning **Before opening the chassis, disconnect the telephone-network cables to avoid contact with telephone-network voltages.**

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

Warning **This unit might have more than one power cord. To reduce the risk of electrical shock, disconnect all power supply cords before servicing the unit.**

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Make sure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. and 240 VAC, 10A international are used on the phase conductors (all current-carrying conductors).**

Warning **This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.**

Warning **Blank faceplates and cover 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, faceplates, front covers, and rear covers are in place.**

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.**

Warning **Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.**

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.**

Warning **Before working on a system that has an On/Off switch, turn OFF the power and unplug the power cord.**

Warning **Read the installation instructions before you connect the system to its power source.**

Warning **The ports labeled "10BaseT," "100BaseTX," and "10/100" are safety extra-low voltage (SELV) circuits. SELV circuits should only be connected to other SELV circuits. Avoid connecting these circuits to telephone network voltage (TNV) circuits.**

Warning **There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.**

General Precautions

Observe the following general precautions when using and working with your system:

- Keep your system components away from radiators and heat sources, and do not block cooling vents.
- Do not spill food or liquids on your system components, and never operate the product in a wet environment. If the computer gets wet, see the appropriate chapter in your troubleshooting guide or contact the Cisco Technical Assistance Center (TAC). For instructions on contacting TAC, see the "Obtaining Technical Assistance" section on page xxi.
- Do not push any objects into the openings of your system components. Doing so can cause fire or electric shock by shorting out interior components.

- Position system cables and power cables carefully; route system cables and the power cable and plug so that they cannot be stepped on or tripped over. Be sure that nothing rests on your system component cables or power cable.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local and national wiring rules.
- To help avoid possible damage to the system board, wait 5 seconds after turning off the system before removing a component from the system board or disconnecting a peripheral device from the computer.

Maintaining Safety with Electricity

Follow these guidelines when working on equipment powered by electricity:

- If any of the following conditions occur, contact the Cisco Technical Assistance Center (TAC):
  - The power cable, extension cable, or plug is damaged.
  - An object has fallen into the product.
  - The product has been exposed to water.
  - The product has been dropped or damaged.
  - The product does not operate correctly when you follow the operating instructions.
- Use the correct external power source. Operate the product only from the type of power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult TAC or a local power company.
- Use only approved power cables. If you have not been provided with a power cable for your computer or storage system or for any AC-powered option intended for your system, purchase a power cable that is approved for use in your country. The power cable must be rated for the product and for the voltage and current marked on the product’s electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the product.
- To help prevent electric shock, plug the VLAN Policy Server, components, and peripheral power cables into properly grounded electrical outlets. These cables are equipped with three-prong plugs to help ensure proper grounding.

Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a three-wire cable with properly grounded plugs.

- Observe extension cable and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80% of the extension cable with the properly grounded plugs.
- To help protect your system and components from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptable power supply (UPS).
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local and national wiring rules.

Protecting Against Electrostatic Discharge

Static electricity can harm delicate components inside your computer. To prevent static damage, discharge static electricity from your body before you touch any of your computer's electronic components, such as the microprocessor. You can discharge static electricity by touching an unpainted metal surface on the computer chassis.

As you continue to work inside the computer, periodically touch an unpainted metal surface to remove any static charge your body may have accumulated.

You can also take the following steps to prevent damage from electrostatic discharge (ESD):

- When unpacking a static-sensitive component from its shipping carton, do not remove the component from the antistatic packing material until you are ready to install the component in your computer. Just before unwrapping the antistatic packaging, be sure to discharge static electricity from your body.
- When transporting a sensitive component, first place it in an antistatic container or packaging.
- Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads and workbench pads.

Preventing EMI

When you run wires for any significant distance in an electromagnetic field, electromagnetic interference (EMI) can occur between the field and the signals on the wires.

Note that:

- Bad plant wiring can result in radio frequency interference (RFI).
- Strong EMI, especially when it is caused by lightning or radio transmitters, can destroy the signal drivers and receivers in the system, and can even create an electrical hazard by conducting power surges through lines and into the system.

To predict and remedy strong EMI, consult RFI experts.

Preparing Your Site for Installation

This section describes the requirements your site must meet for safe installation and operation of your VLAN Policy Server. Ensure that your site is properly prepared before beginning installation.

Environmental

When planning your site layout and equipment locations, keep in mind the precautions described in this section to help avoid equipment failures and reduce the possibility of environmentally caused shutdowns. If you are currently experiencing shutdowns or unusually high errors with your existing equipment, these precautions will help you isolate the cause of failures and prevent future problems.

Use the following precautions when planning the operating environment for your VLAN Policy Server.

- Always follow the ESD-prevention procedures described in the "Preventing EMI" section on page 7 to avoid damage to equipment. Damage from static discharge can cause immediate or intermittent equipment failure.
- Make sure that the chassis cover is secure. The chassis is designed to allow cooling air to flow effectively within it. An open chassis allows air leaks, which could interrupt and redirect the flow of cooling air from internal components.
- Electrical equipment generates heat. Ambient air temperature might not be adequate to cool equipment to acceptable operating temperatures without adequate circulation. Make sure that the room in which you operate has adequate air circulation.

Choosing a Site for Installation

⚠ **Warning** **This unit is intended for installation in restricted access areas. A restricted access area is where access can only be gained by service personnel through the use of a special tool, lock and key, or other means of security, and is controlled by the authority responsible for the location.**

- Choose a site with a dry, clean, well-ventilated and air-conditioned area.
- Choose a site that maintains an ambient temperature of 10° to 35°C (50° to 95°F).

Grounding the System

⚠ **Warning** **Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.**

Creating a Safe Environment

Follow these guidelines to create a safe operating environment:

- Keep tools and chassis components off the floor and away from foot traffic.
- Clear the area of possible hazards, such as moist floors, ungrounded power extension cables, and missing safety grounds.
- Keep the area around the chassis free from dust and foreign conductive material (such as metal flakes from nearby construction activity).

AC Power

Ensure that the plug-socket combination is accessible at all times, because it serves as the main disconnecting device. For VLAN Policy Server power requirements, see Appendix B, "Technical Specifications."

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Make sure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. and 240 VAC, 10A international are used on the phase conductors (all current-carrying conductors).**

Cabling

Use the cables in the accessory kit to connect the VLAN Policy Server console port to a console or computer that is running a console program. In addition to the console cable, you must supply your own standard Ethernet cable to connect the VLAN Policy Server to your network. For information detailing cable requirements, see the "Network Cable Requirements" section on page 1-11.

A structured wiring system provides a standardized way to wire a building for all types of networks for the VLAN Policy Server to be installed. The main distribution frame links all the building's interior wiring and provides an interface connection to circuits coming from outside sources such as the local telephone company. Wiring hubs (peripherals for cabling installations) provide the connection logic unique to Fast Ethernet cables that the VLAN Policy Server uses.

Unshielded twisted pair (UTP) copper wire is used to connect the VLAN Policy Server and distributes the network connections to wall jacks near each piece of network equipment.

Precautions for Rack Mounting

Observe the following precautions for rack stability and safety. Also refer to the rack installation documentation accompanying the rack for specific warning and/or caution statements and procedures.

Servers, storage systems, and appliances are considered to be components in a rack. Thus, “component” refers to any server, storage system, or appliance, as well as to various peripherals or supporting hardware.

- Do not move large racks by yourself. Due to the height and weight of the rack, a minimum of two people are needed to accomplish this task.
- Ensure that the rack is level and stable before extending a component from the rack.
- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.
- Ensure that proper airflow is provided to components in the rack.
- Do not step on or stand on any system or component when servicing any other system or components in a rack.
- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:**

Precautions for Products with Telecommunications Options

Observe the following guidelines when working with telecommunications options:

- Do not connect or use a modem or telephone during a lighting storm. There may be a risk of electrical shock from lightning.
- Never connect or use a modem or telephone in a wet environment.
- Do not plug a modem or telephone cable into the Ethernet connector.
- Disconnect the modem cable before opening a product enclosure, touching or installing internal components, or touching an uninsulated modem cable or jack.
- Do not use a telephone line to report a gas leak while you are in the vicinity of the leak.

Required Tools and Equipment

You need the following tools and equipment to install the VLAN Policy Server:

- Console cable
- Power cord
- Number 2 Phillips screwdriver
- Tape measure and level
- Antistatic mat or antistatic foam
- ESD grounding strap
- Ethernet cables
- Rack-mount kit
  - Two chassis-support brackets
  - Two rack-mount brackets
  - Six screws

Installing and Configuring the VLAN Policy Server

This chapter describes how to install and configure the VLAN Policy Server. It contains the following sections:

Quick Reference

Table 3-1 provides a high-level overview of the installation process.

Table 3-1 Quick Reference

Task	Steps	References
Install the VLAN Policy Server.	**1.** Attach the chassis support brackets to the chassis. **2.** Attach the rack-mount brackets to the rack. **3.** Put the chassis into the rack. **4.** Fasten the chassis in the rack.	Installing the VLAN Policy Server, page 3-3
Connect to a power source.	Connect to an AC power source.	Connecting to the Power Source, page 3-8
Connect cables.	**1.** Plug the network connection into the Ethernet 0 port. **2.** Connect a terminal to the console port.	Connecting Cables, page 3-9
Power on the VLAN Policy Server.	Press the power switch.	Powering On the VLAN Policy Server, page 3-9
Configure the VLAN Policy Server.	**1.** Boot the VLAN Policy Server and log on. **2.** Configure VLAN Policy Server connectivity by responding to the first set of prompts. **3.** Configure discovery by responding to the second set of prompts. **4.** Create a self-signed certificate by responding to the third set of prompts.	Configuring the VLAN Policy Server, page 3-10

Table 3-1 Quick Reference (continued)

Task	Steps	References
Verify the configuration.	1. Log on at the system console. 2. If you are using name resolution, verify that the VLAN Policy Server can resolve hostnames. 3. Verify that the VLAN Policy Server can communicate with the network. 4. Verify that the configuration is correct. 5. Verify that the system time and date are correct.	Verifying the Configuration, page 3-16
Configure the Web browser.	1. Verify that the client system is using a supported browser. 2. Enable JavaScript. 3. Configure the browser to accept all cookies.	Configuring the Web Browser, page 3-17
Verify HTTP and HTTPS connectivity.	Verify that you can connect to the VLAN Policy Server via HTTP and HTTPS.	Verifying HTTP and HTTPS Connectivity, page 3-19

Installing the VLAN Policy Server

This section provides instructions for installing the VLAN Policy Server in a rack. The rack must be properly secured to the floor, to the ceiling or upper wall, and where applicable, to adjacent racks. The rack should be secured using floor and wall fasteners and bracing specified or approved by the rack manufacturer or by industry standards. Refer to the rack manufacturer’s installation documentation for warnings and precautionary information before attempting to install the VLAN Policy Server.

Before installing the VLAN Policy Server in a rack, read the "Preparing Your Site for Installation" section on page 2-7 to familiarize yourself with the proper site and environmental conditions. Failure to read and follow these guidelines could lead to an unsuccessful installation and possible damage to the system and components. Perform the steps below when installing and servicing the VLAN Policy Server:

- Disconnect all power and external cables before installing the system.
- Install the system in compliance with your local and national electrical codes:
  - United States: National Fire Protection Association (NFPA) 70; United States National Electrical Code.
  - Canada: Canadian Electrical Code, Part, I, CSA C22.1.
  - Other countries: If local and national electrical codes are not available, refer to IEC 364, Part 1 through Part 7.
- Do not work alone under potentially hazardous conditions.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Do not attempt to install the VLAN Policy Server in a rack that has not been securely anchored in place. Damage to the system and personal injury may result.
- Because of the size and weight of the computer system, never attempt to install the computer system by yourself.

Warning **Before working on a system that has an on/off switch, turn OFF the power and unplug the power cord.**

Warning **Do not touch the power supply when the power cord is connected. For systems with a power switch, line voltages are present within the power supply even when the power switch is off and the power cord is connected. For systems without a power switch, line voltages are present within the power supply when the power cord is connected.**

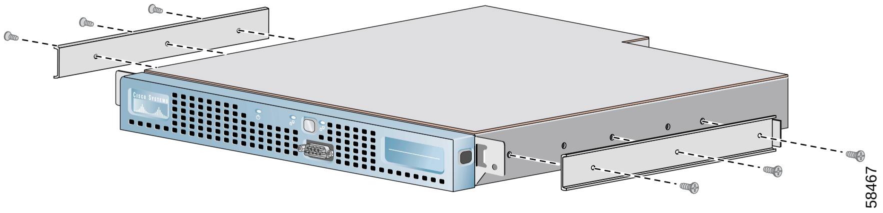
See Chapter 2, "Preparing for Installation," for additional safety information regarding installing the VLAN Policy Server.

Installing the VLAN Policy Server in a Rack

To install the VLAN Policy Server in a rack, perform the following steps:

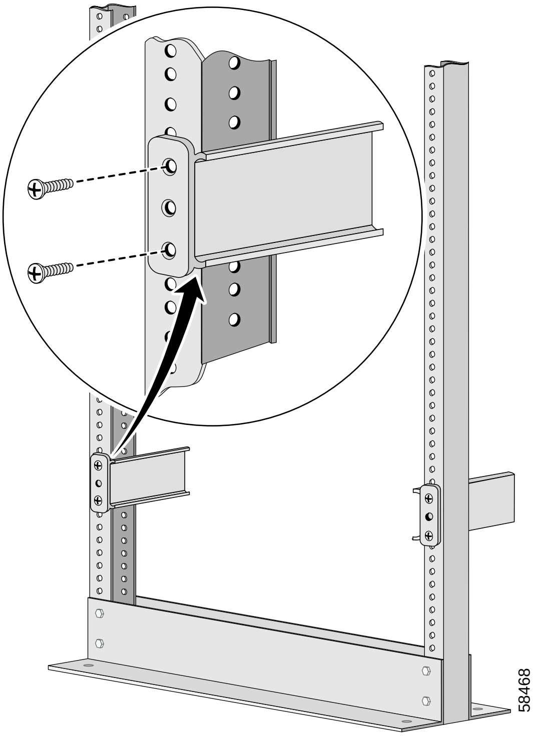
Step 1 Attach chassis-support brackets—Use the screws provided to attach one chassis-support bracket to each side of the chassis. Use the three front screw holes on the VLAN Policy Server, and use three screws on each side. See Figure 3-1.

Figure 3-1 Chassis-Support Bracket Installation



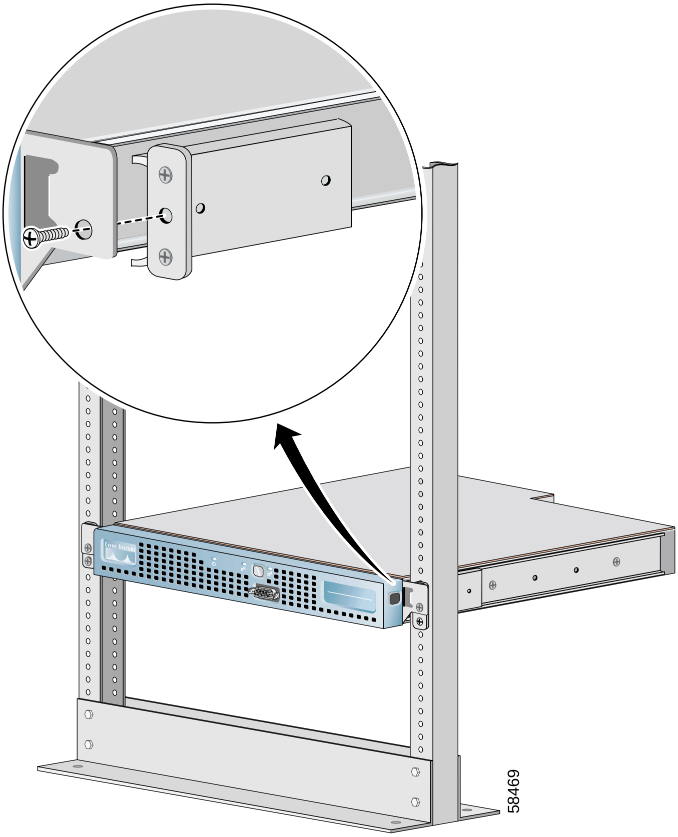
Step 2 Attach the rack-mount brackets to the rack—Because not all holes in a rack are equidistant, it is possible to misalign the brackets. To avoid this problem, make sure that the three holes of the brackets line up exactly with the holes in the rack. Screws are not provided. See Figure 3-2.

Figure 3-2 Rack-Mount Bracket Installation



Step 3 Put the chassis into the rack—Slide the chassis-support brackets (attached to the chassis in step 1) into the rack-mount brackets (attached to the rack in step 2). See Figure 3-3.

Figure 3-3 Chassis Installation



Step 4 Fasten the chassis in the rack—Fasten the flanges of the chassis to the rack. When you are done, the chassis should not slide on the channel bar.

Caution The rack-mount kit is not intended for use as a slide rail system. You must complete installation of the front-mount bracket assembly by securely fastening the chassis into the rack.

Connecting to the Power Source

Warning **Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.**

Warning **Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.**

Connect the AC power receptacle to the AC power source with the provided power cable.

Connecting Cables

Use unshielded twisted pair (UTP) copper wire Ethernet cable, with standard RJ-45 compatible plugs, to connect the VLAN Policy Server to the network.

To connect the cables:

Step 1 Plug the network connection into the Ethernet 0 port. For the location of the Ethernet 0 port, see Figure 1-3.

Step 2 Connect a console to the console port (the front serial port). To connect the console to the terminal port:

a. Attach a DB-9 to RJ-45 adapter (provided) to the serial port on the console.

b. Attach a DB-9 to RJ-45 adapter (provided) to the console port on the VLAN Policy Server.

c. Connect the console to the VLAN Policy Server using an RJ-45 cable (provided).

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.**

Powering On the VLAN Policy Server

To turn the VLAN Policy Server power on, press the power switch. To turn power off, press and hold the power switch for at least four seconds. There is a power switch on both the bezel and the front panel.

The system begins booting and sends messages to the console window. When the logon prompt appears, you can configure the system.

Configuring the VLAN Policy Server

Configure the VLAN Policy Server when you boot the system for the first time, and whenever you manually erase the configuration using the **erase config** command (for more information, refer to the "erase config" section on page C-20).

Press the **Backspace** key or the **Delete** key to delete characters when entering a response to a prompt. You cannot edit a response after you press the **Enter** key. To change an entered response you must exit the setup program and enter your response again.

You can exit the setup program in one of the following two ways:

- Press **Ctrl-c**.

  The logon prompt appears. Log on as the user setup to run the setup program.

- Enter **no** at the final prompt:

  ```
  Would you like to save this configuration? [yes].
  ```

  The setup program exits without saving the configuration, then restarts.

To configure the VLAN Policy Server, perform the following steps:

Step 1 Power on the VLAN Policy Server.

When the system finishes booting, a logon prompt appears on the console.

Step 2 At the logon prompt, enter **setup**.

When you boot the system for the first time, it is not configured. Logging on as **setup** allows you to configure the system.

Step 3 Enter responses to the first set of prompts to configure VLAN Policy Server connectivity. Table 3-2 describes how to respond to the prompts.

Table 3-2 General Configuration

Prompt	Response Description	Sample Response
`login:`	Enter **`setup`**.	**setup**
`host name:`	System hostname.	**SolutionEngine**
`domain name:`	System domain name.	**cisco.com**
`<admin> password:`	Sets the password for the default user **admin**. Characters you type do not appear on screen. **Note** Default user **admin** is reserved and cannot be deleted or changed.	**wq1Cvu2pl**
`confirm passwords`	Reenter password to verify that you typed it correctly. Characters you type do not appear on screen.	**wq1Cvu2pl**
`eth0 ip address:`	IP address of Ethernet 0 interface.	**209.165.200.224**
`eth0 network mask:`	Network mask of Ethernet 0 interface.	**255.255.255.224**
`default gateway ip address:`	IP address of default router that connects VLAN Policy Server to network.	**209.165.200.224**
`DNS server ip address:`	IP address of DNS server that VLAN Policy Server uses for name/address resolution. The setup program does not validate the IP address you enter. If you are not using a DNS server, see the "Configuring the VLAN Policy Server Without a DNS Server" section on page 3-15 for instructions before proceeding.	**209.165.201.1**
`Would you like to save this configuration? [yes]:`	One of the following: • Type **`yes`** and press **Enter** to save the configuration. The configuration is saved and system reboots. • Type **`no`** and press **Enter** to exit without saving configuration and run setup program again.	**Enter**

Step 4 Answer the next set of prompts to configure discovery. Table 3-3 describes how to respond to the prompts. Entering the default at each prompt will cause the VLAN Policy Server to discover the entire network. Answers to these prompts are not required; you can initiate discovery at a later time using the web interface. To skip this part of the configuration, enter `no` at the first prompt.

For more information on discovery, including instructions on initiating discovery and adding seed devices, see the VLAN Policy Server online help by selecting **Help** > **Performing Administrative Tasks** > **Discovery: Overview** in the VLAN Policy Server web interface.

Table 3-3 Discovery Configuration

Prompt	Response Description	Sample Response
`Do you want to set up discovery now (y/n)? [Default n]:`	Enter `yes` to configure discovery. Enter `no` to skip this procedure. You can initiate discovery through the web interface at a later time.	**yes**
`Enter list of seed devices [Default 127.0.0.1]:`	Enter the IP addresses of the seed devices you want the VLAN Policy Server to discover, with a colon between each address. Verify that all seed devices are reachable from the VLAN Policy Server.	**209.165.200.224**
`Enter the network device or range of device addresses [Default *.*.*.*]:`	The discovery tool uses simple network management protocol (SNMP) to communicate with network devices. This step, along with the next two steps, will set up the SNMP community strings used by the VLAN Policy Server to access the network devices. Enter the range of device addresses to be discovered.	**209.165.201.[1-30]**
`Enter the read community string for *.*.*.* [Default Public]:`	Enter the read community string for each of the network devices entered.	**public**
`Enter the read/write community string for *.*.*.* [Default Public]:`	Enter the read/write community string for each of the network devices entered.	**public**
`Do you want to add more (y/n) [Default n]:`	Enter `yes` to add more devices, or enter `no` if the list of devices is complete.	**no**

Table 3-3 Discovery Configuration (continued)

Prompt	Response Description	Sample Response

`Select one of the following`
`1) Discover devices only in these ranges`
`2) Do not discover devices in these ranges`
`Enter the number corresponding to the option you have chosen or q to quit [Default q]:`
	This step and the next provide the filters to define the discovery area.
	Enter **`1`**, **`2`**, or **`q`** as appropriate. If you enter 1 or 2, you will be prompted for the ranges in the next step. If you enter q, you will skip to the last step.
		1

`Enter the IP address or range of IP addresses to limit discovery with ':' as delimiter:`	Enter a range of devices to limit discovery.	**209.165.200.[225-254]**
`Do you want to proceed (y/n) [Default y]:`	The VLAN Policy Server displays the information you have entered. Enter **`yes`** if the information presented is correct.	**yes**

Step 5 Answer the next set of prompts to create a self-signed certificate. This certificate will allow you to access the VLAN Policy Server securely, using HTTPS, until you obtain a certificate from a certificate authority (CA). Table 3-4 describes how to respond to the prompts. After you finish responding to the prompts, the VLAN Policy Server will reboot.

Table 3-4 Self-Signed Certificate Creation

Prompt	Response Description	Sample Response
`Country Name`	Enter a 2-character code.	**US**
`State or Province Name`	Enter the full name of a state or province.	**Snake Desert**
`Locality Name`	Enter a city or locality name.	**Snake Town**
`Organization Name`	Enter a company name.	**Snake Oil, LTD.**
`Organizational Unit`	Enter the section of the company that is using the VLAN Policy Server.	**Webserver Team**
`Common Name`	Enter a fully qualified domain name (FQDN).	**www.snakeoil.dom**
`Email Address`	Enter an email address.	**www@snakeoil.dom**

If you want to change the information in the configuration, use the following CLI commands:

- To change the hostname, use the **hostname** command (see hostname, page C-23).
- To change the domain name, use the **ip domain-name** command (see ip domain-name, page C-29).
- To change the DNS server, or add up to 2 other DNS servers, use the **ip name-server** command (see ip name-server, page C-30).
- To configure or reconfigure an ethernet port, use the **interface** command (see interface, page C-28).

If you want to change any other part of the VLAN Policy Server configuration, use the **erase config** command to erase the previous configuration (see erase config, page C-20), and run the setup program again.

Name Resolution

The VLAN Policy Server resolves hostnames by using a Domain Name System (DNS) server, or by using the **import** CLI command. If you are using a DNS server, register the system in DNS on a DNS server. Use the VLAN Policy Server hostname as its DNS name. If you plan to use the **import** command, refer to the "import" section on page C-24.

The VLAN Policy Server does not require name resolution, but if it is not used, the following problems are among those that will occur:

- Hostnames will not resolve.
- Discovery will be slow.
- Connecting to the VLAN Policy Server via Telnet will be slow. You will be able to connect to the VLAN Policy Server only after name resolution on the client times out.
- Ping and traceroute commands will result in 100% packet losses in 4 out of 5 ICMP packets. This occurs because the VLAN Policy Server times out when attempting reverse DNS lookup.
- IP addresses will appear in hostname columns.

Configuring the VLAN Policy Server Without a DNS Server

If you are not using a DNS server, perform the same steps described in the "Configuring the VLAN Policy Server" section on page 3-10, substituting Step 1 and Step 2 in the procedure with the following:

Step 1 At the `DNS server ip address:` prompt, enter any IP address.

Step 2 After you finish configuring the VLAN Policy Server, erase the IP address you entered by entering the following CLI command:

```
no ip name-server ip-address
```

where *ip-address* is the IP address you entered at the `DNS server ip address:` prompt. For more information, see the "ip name-server" section on page C-30.

Verifying the Configuration

While at the console, verify that the VLAN Policy Server is correctly configured by performing the following steps:

Step 1 At the system console, enter **admin** at the Login prompt, and enter the password you created at the Password prompt during setup.

If you cannot log on, refer to the "Cannot Log On to the System" section on page A-2 for troubleshooting information.

Step 2 Enter the following command to verify that the system can communicate with the network:

```
# ping ip-address
```

where *ip-address* is the IP address of a host that is accessible on the network. A DNS server is an excellent host to ping because it should always be running and accessible. For information about the ping command, refer to the "ping" section on page C-9.

If the system cannot communicate with the network, refer to the "VLAN Policy Server Cannot Connect to the Network" section on page A-2 for troubleshooting information.

Step 3 If you are using a DNS server, enter the following command to verify that the VLAN Policy Server can obtain DNS services from the network:

```
# nslookup dns-name
```

where *dns-name* is the DNS name of a host that is registered in DNS. If the browser cannot obtain the IP address of the host from DNS, make sure that the hostname has been configured in the DNS server. Then enter the **ip name-server** command to specify that DNS server for address resolution. Refer to the "ip name-server" section on page C-30 for instructions.

Step 4 Enter the command **show config** to verify that the configuration is as you expected. Refer to the "show config" section on page C-50 for information about this command.

Step 5 Enter the `show clock` command to verify that the system time and date are correct in Coordinated Universal Time (UTC). If the time or date is incorrect, set the correct time and date. If your network uses Network Time Protocol (NTP), configure the system to use NTP. The NTP server will set the date and time.

For more information about configuring time and date, refer to the "Setting System Date and Time" section on page 4-6.

Step 6 Enter the **exit** command to log off of the system.

Configuring the Web Browser

Before you connect to the VLAN Policy Server via its web interface, make sure your browser is properly configured.

To configure Netscape Navigator, perform the following steps:

Step 1 Verify that the client system is running one of the following:

- Netscape Navigator 4.78.
- Japanese Netscape 4.75, on Japanese Windows 2000 or Japanese Windows NT.

Step 2 Enable JavaScript:

a. Select **Edit** > **Preferences** > **Advanced**.

b. Select **Enable JavaScript** checkbox.

c. Click **OK**.

Step 3 Configure Netscape to Navigator accept all cookies:

a. Select **Edit** > **Preferences** > **Advanced**.

b. Select the **Accept all cookies** radio button.

c. Click **OK**.

Step 4 Change the default font to a sans serif font for improved readability:

a. Select **Edit** > **Preferences** > **Appearance** > **Fonts**.

b. In the **Variable Width Font** and **Fixed Width Font** selection areas, select a sans-serif font (for example, Arial) and a font size.

c. Click **OK**.

The text in the browser window is redrawn using the new fonts.

To configure Internet Explorer, perform the following steps:

Step 1 Verify that the client system is running one of the following:

a. Internet Explorer 5.5 with Service Pack 2

b. Japanese Microsoft Internet Explorer 5.5 with Service Pack 1, on Japanese Windows 2000 or Japanese Windows NT.

Step 2 Enable JavaScript:

a. Select **Tools** > **Internet Options** > **Security.**

b. Make sure that the Internet icon is selected, and click **Custom Level**.

c. Select **Enable active scripting, Allow paste operations via script**, and **Scripting of Java applets**.

Step 3 Configure your browser to accept all cookies:

a. Select **Tools** > **Internet Options** > **Security**.

b. Make sure that the Internet icon is selected, and click **Custom Level**.

c. Scroll to Cookies. Select enable for both “Allow cookies that are stored on your computer,” and “Allow per-session cookies (not stored).”

d. Click **OK**.

Step 4 Change the default font to sans serif for improved readability:

a. Select **Tools** > **Internet Options**. A dialog box appears.

b. Click the **General** tab, and select **Fonts**. A second dialog box appears.

c. From the **Web page font** and **Plain text font** lists, select a sans-serif font (for example, Arial).

d. Click **OK** in both dialog boxes to close them.

The text in the browser window is redrawn using the new fonts.

Verifying HTTP and HTTPS Connectivity

To verify HTTP and HTTPS connectivity, connect to the VLAN Policy Server using a Web browser and perform the following steps:

Step 1 To verify HTTP connectivity, enter the system IP address in a web browser, followed by `:1741` (the default port number).

For example, if the system IP address is 209.165.202.128, enter

`http://209.165.202.128:1741`.

If a logon dialog box appears, you have connectivity. If you cannot connect to the VLAN Policy Server, see the "Cannot Connect to the VLAN Policy Server Using a Web Browser" section on page A-4.

Step 2 To verify HTTPS connectivity, enter the system IP address in a web browser, prefixed by https. No port number is needed.

For example, if the system IP address is 209.165.202.128, enter

`https://209.165.202.128`.

If a logon dialog box appears, you have connectivity. If you cannot connect to the VLAN Policy Server, see the "Cannot Connect to the VLAN Policy Server Using a Web Browser" section on page A-4.

CHAPTER 4

Administering the VLAN Policy Server

This chapter describes the VLAN Policy Server's major system administration tasks. It contains:

Logging On and Off the System

You can connect to the VLAN Policy Server system in the following ways:

- Point a web browser to the VLAN Policy Server.
- Telnet to the system.
- Connect a console to the VLAN Policy Server console port.

If you are connected to the VLAN Policy Server through the web, enter a valid username and password in the logon screen to log on, and click the Logout button to log off. If you are connected to the VLAN Policy Server through the command-line interface (CLI), enter a valid username and password at the logon prompt to log on, and enter the **exit** command to log off.

Logging On to the VLAN Policy Server Using a Web Browser

The VLAN Policy Server provides a web interface for performing administrative tasks.

Note For detailed information on performing administrative tasks, see the online help that is provided with the web interface.

To log on to the VLAN Policy Server using a web browser:

Step 1 Open a web browser.

Step 2 Enter the system IP address in the web browser, followed by **:1741** (the default port number).

For example, if the system IP address is 209.165.202.128, enter

http://209.165.202.128:1741.

The logon dialog box appears.

Step 3 Enter the username.

Step 4 Enter the password.

Step 5 Click **Login**.

The VLAN Policy Server web interface opens.

Administering User Accounts

The VLAN Policy Server allows you to create users with tiered access. For more information on creating and administering user accounts, refer to the VLAN Policy Server online help. To access this information in the online help, perform the following steps:

Step 1 Point a browser to the VLAN Policy Server, and log on.

Step 2 Click **Help** in the upper-right corner of the screen. The Help screen appears.

Step 3 Select **Tiered Access** > **Managing User Account Profiles**.

Backing Up and Restoring Your VLAN Policy Server

The VLAN Policy Server should be backed up at regular intervals. Before attempting to back up or restore your VLAN Policy Server, make sure the username and password are valid on the target system, the target directory exists and has the proper permissions for the username and password, and the system allows FTP. Backing up the VLAN Policy Server will preserve all domains, roles, users, and discovery configuration information.

To back up your VLAN Policy Server, perform the following steps:

Step 1 Point a browser to the VLAN Policy Server, and log on.

Step 2 Select **Administration** > **Software** > **BackUp/Restore**.

Step 3 If you have not yet configured the backup location, do so by clicking the **Configure** button and entering the required information.

Step 4 Click the **Backup** button.

To restore your VLAN Policy Server, perform the following steps:

Step 1 Point a browser to the VLAN Policy Server, and log on.

Step 2 Select **Administration** > **Software** > **Backup/Restore**.

Step 3 Click the **Restore** button.

Step 4 From the drop-down list, select the image you want to restore, and click **Continue**.

Step 5 A window appears, displaying the image you will be restoring. If the information is correct, click **OK**.

You can also back up and restore your VLAN Policy Server by using the following CLI commands:

- **backup**—Use this command to back up your VLAN Policy Server. For more information, see the "backup" section on page C-17.
- **backupconfig**—Use this command to configure your VLAN Policy Server backup location. For more information, see the "backupconfig" section on page C-17.
- **restore**—Use this command to restore your VLAN Policy Server. For more information, see the "restore" section on page C-40.

Shutting Down and Reloading the VLAN Policy Server

The VLAN Policy Server can be shut down using either the Web interface or the CLI. Rebooting the system starts the management services installed on the system, even if they were stopped prior to the reboot.

To restart the VLAN Policy Server using the web interface, select **Administration** > **Restart.** Click **Yes** in the dialog box that appears. The VLAN Policy Server will restart.

To shut down the VLAN Policy Server using the CLI, enter the **`shutdown`** command before powering off the VLAN Policy Server. If you power off the VLAN Policy Server without entering this command, you might disable the system.

To reboot the system using the CLI, enter the **`reload`** command. The logon prompt appears when the reboot is complete.

To erase the system configuration and reboot the system using the CLI, enter the **`erase config`** command. After the system reboots, you must reconfigure the system using the setup program, as described in the "Configuring the VLAN Policy Server" section on page 3-10.

For more information about these commands, refer to:

- The "shutdown" section on page C-66
- The "reload" section on page C-35
- The "erase config" section on page C-20

Setting System Date and Time

The VLAN Policy Server uses Universal Coordinated Time (UTC) for keeping the time and date. The VLAN Policy Server uses client local time to display the time and date when connected through the Web interface. It uses UTC to display the time and date when connected through Telnet or a console, or when viewing log files.

You can set and maintain the system date and time using either of two methods:

- Use the **ntp server** CLI command to assign one or more network time protocol (NTP) servers with which the system will synchronize its date and time. *This method is recommended*. For more information, see the "Setting Date and Time Using NTP" section on page 4-6.
- Use the clock CLI command to set the date and time manually, updating it as needed. For more information, see the "Setting Date and Time Manually" section on page 4-7.

To display the system time, enter the **show clock** command. For more information, see the "show clock" section on page C-10.

Setting Date and Time Using NTP

NTP is the recommended method for configuring time and date on the system. If your network uses NTP to set the date and time on devices, enter the following command in the CLI to designate an NTP server for the system to use to set the system clock:

```
# ntp server ip-address
```

where *ip-address* is the IP address of an NTP server.

For more information, refer to the "ntp server" section on page C-33.

If you disable NTP, set the system clock to UTC manually as described in the "Setting Date and Time Manually" section on page 4-7. If you do not set the system clock manually after disabling NTP, the system clock might be inaccurate when the system is rebooted.

Setting Date and Time Manually

If your network does not use NTP to set the system time on devices and the time is not set correctly, set the date and time to UTC manually by entering the following command in the CLI:

```
# clock set hh:mm:ss month day year
```

where *hh***:***mm***:***ss* is the current time (for example, 13:32:00), *month* is the current month (for example, January, February), *day* is the day of the month (for example, 31), and *year* is the current year (for example, 2001).

For more information, refer to the "clock" section on page C-19.

Configuring the Ethernet Ports

The VLAN Policy Server uses 10/100 Mbps Ethernet connectors. The Ethernet 0 interface is configured when the VLAN Policy Server is configured. To enable or change an additional interface configuration, enter the **interface** command in the CLI. For instructions about using the interface command, refer to the "interface" section on page C-28.

Any VLAN Policy Server Ethernet port can be individually configured to allow connections through the following protocols:

- Cisco Discovery Protocol (CDP)
- Hypertext transfer protocol (HTTP)
- Hypertext transfer protocol secure (HTTPS)
- Internet Control Message Protocol (ICMP)
- Secure shell (SSH) 1 and 2
- Simple network management protocol (SNMP)
- Telnet

To enable CDP on an individual Ethernet port, use the **cdp** command. For more information, see the "cdp" section on page C-18. To disable any of the other protocols listed above on an individual Ethernet port, use the **firewall** command. For more information about the **firewall** command, including a detailed example of its use, see the "firewall" section on page C-21.

Administering Management Services

The VLAN Policy Server allows you to administer all management services simultaneously. All commands that affect management services affect all of them simultaneously; the logs that collect services information collect information about all of them.

You can stop and restart the management services if the system is not responding correctly to a management application. This should cause the services to reset and function properly again. Management services are restarted automatically when you reboot.

To stop management services, enter the following command in the CLI:

```
# services stop
```

To start management services, enter the following command in the CLI:

```
# services start
```

To view management services status, enter the following command in the CLI:

```
# services status
```

For more information about the services command, refer to the "services" section on page C-42.

Viewing System Information

To view system information, use the **show** commands, such as **show clock** and **show process**. For more information on the **show** commands, see Appendix C, "Command Reference."

Using the Maintenance Image

The VLAN Policy Server has an operating system image and a default system configuration (hereafter collectively called the maintenance image) stored in Flash memory. You can use the maintenance image to boot the system when you need to perform some system administration tasks and disaster recovery.

You can run only the following commands while the system is running from the maintenance image: **reload**, **erase config**, and **fsck**.

For information about these commands, refer to the "Maintenance Image Commands" section on page C-71.

While the maintenance image is running, you can do the following tasks, which you cannot do when the system is booted from the disk:

- Recover from loss of all administrative user account passwords.
- Perform disk filesystem integrity checks.

Booting from the Maintenance Image

As a security measure, you can boot from the maintenance image only while connected to the system console.

Step 1 Connect a console to the VLAN Policy Server console port, and log on as **admin**.

Step 2 Reboot the system by doing one of the following:

- If the system is running, reload it. Refer to the "reload" section on page C-35 for instructions.
- If the system is powered off, power it on.
- If you cannot log on because you have lost all user account passwords, power the system off and then back on.

Step 3 When the `LILO boot:` prompt appears, press the Tab key.

Step 4 When the `boot:` prompt appears, enter **`CiscoBreR`**.

Step 5 After you complete all necessary tasks, reboot the system by entering the **`reload`** command, and allow the system to boot from the disk.

Recovering from the Loss of All Administrator Passwords

If you cannot log on to the system because you cannot remember the administrator account names or passwords, you can recover by booting from the maintenance image, erasing the existing configuration from Flash memory, and reconfiguring the system using the setup program.

To recover from the loss of all administrator passwords:

Step 1 Boot the system from the maintenance image as described in the "Booting from the Maintenance Image" section on page 4-9.

Step 2 Enter the **`erase config`** command to erase the system configuration. The system reboots.

Step 3 Allow the system to boot from disk.

Step 4 Configure the system from the setup program, as described in the "Configuring the VLAN Policy Server" section on page 3-10.

Step 5 After the system reboots, reconfigure the VLAN Policy Server by following the steps outlined in the "Installing the VLAN Policy Server" section on page 3-3.

Installing a Replacement VLAN Policy Server

This section describes tasks you should perform when installing a replacement VLAN Policy Server (a new unit intended to replace an existing unit), to make the transition as easy as possible. These tasks are in addition to the installation and configuration processes described in Chapter 3, "Installing and Configuring the VLAN Policy Server."

Preparing to Install the Replacement VLAN Policy Server

Before removing the old VLAN Policy Server:

Step 1 Enter the command **`show config`** in the CLI to view the VLAN Policy Server configuration.

Step 2 Record the old VLAN Policy Server configuration settings, so you can configure the new VLAN Policy Server using these settings.

Step 3 Back up the old VLAN Policy Server. See the "Backing Up and Restoring Your VLAN Policy Server" section on page 4-3 for details.

Step 4 Enter the **`shutdown`** command.

The system shuts down.

Installing the Replacement VLAN Policy Server

To install the replacement VLAN Policy Server:

Step 1 Install and power on the new VLAN Policy Server:

a. Install the VLAN Policy Server (see the "Installing the VLAN Policy Server" section on page 3-3).

b. Connect to a power source (see the "Connecting to the Power Source" section on page 3-8).

c. Connect the cables (see the"Connecting Cables" section on page 3-9).

d. Power on the VLAN Policy Server (see the "Powering On the VLAN Policy Server" section on page 3-9).

Step 2 Run the setup program (see the "Configuring the VLAN Policy Server" section on page 3-10).

Step 3 Use the configuration settings that you recorded from the old system to respond to the setup program prompts.

Step 4 Restore the information saved when you backed up the old system. For more information, see the "Backing Up and Restoring Your VLAN Policy Server" section on page 4-3.

Using the Recovery CD

A recovery CD is included with your VLAN Policy Server. With this CD, you can reimage the VLAN Policy Server, or you can boot from the Rescue image.

Note Although every effort has been made to validate the accuracy of the software version on the recovery CD, after you reimage your VLAN Policy Server, you must review the related software downloads on http://www.cisco.com for any software updates.

Reimaging the VLAN Policy Server

Use the VLAN Policy Server Recovery CD to reimage the VLAN Policy Server, should it become necessary. Doing so destroys all data and installs a new image.

To reimage your VLAN Policy Server:

Step 1 Connect a console to the VLAN Policy Server console port. For the location of the console port, see the "Front Panel Features" section on page 1-3.

Step 2 Log on as user administrator, and enter the password created when the VLAN Policy Server was configured.

Step 3 Put the User Registration Tool VPS Recovery CD (version 2.5 Cisco 1101 VLAN Policy Server) in the VLAN Policy Server CD-ROM. For the location of the CD-ROM, see the "Front Panel Features" section on page 1-3.

Step 4 Enter the `reload` command. The VLAN Policy Server reboots. For more information on the reload command, see the "reload" section on page C-35.

Step 5 At the `Do you wish to continue (yes/[no]/rescue):` prompt, enter **`yes`**. If you do not want to reimage your VLAN Policy Server, enter **`rescue`**. For more information about the rescue image, see the "Using the Rescue Image" section on page 4-13.

Step 6 When the VLAN Policy Server ejects the recovery CD, remove it.

Step 7 At the `Do you wish to reload and start the install?(yes/[no]):` prompt, enter **`yes`**. The VLAN Policy Server reboots, and reimaging is completed.

Using the Rescue Image

The rescue image is similar to the maintenance image, but is accessible through the recovery CD. You can use the rescue image to boot the system to perform some system administration tasks and disaster recovery. You can run only the following commands while the system is running from the rescue image: **reload**, **erase config**, and **fsck**.

For more information about how you can use the rescue image, see the related information about the maintenance image in the "Using the Maintenance Image" section on page 4-9.

To boot from the rescue image, perform the following steps:

Step 1 Connect a console to the VLAN Policy Server console port. For the location of the console port, see the "Front Panel Features" section on page 1-3.

Step 2 Log on as the user administrator, using the user administrator password created when the VLAN Policy Server was configured.

Step 3 Put the User Registration Tool VPS Recovery CD (version 2.5 Cisco 1101 VLAN Policy Server) in the VLAN Policy Server CD-ROM. For the location of the CD-ROM, see the "Front Panel Features" section on page 1-3.

Step 4 Enter the `reload` command. The VLAN Policy Server reboots. For more information on the reload command, see the "reload" section on page C-35.

Step 5 At the `Do you wish to continue (yes/[no]/rescue):` prompt, enter **`rescue`**. The VLAN Policy Server boots from the rescue image.

APPENDIX A

Troubleshooting

This appendix provides troubleshooting information. It consists of the following sections:

Cannot Log On to the System

Problem: You cannot log on to the system.

Possible causes:

- You did not run the setup program to create an initial system configuration.
- You lost all the user account passwords.

Resolution:

Step 1 Did you run the setup program after booting the system for the first time?

If no, run the setup program as described in the "Configuring the VLAN Policy Server" section on page 3-10.

If yes, continue.

Step 2 Do you know the password for any system user accounts?

If no, reconfigure the system to create a new user account. Refer to the "Recovering from the Loss of All Administrator Passwords" section on page 4-10 for more information.

If yes, continue.

Step 3 If you are certain you entered a valid username and password, contact the Cisco Technical Assistance Center (TAC) for assistance.

VLAN Policy Server Cannot Connect to the Network

Problem: The system cannot connect to the network.

Possible causes:

- The network cable is not connected to the Ethernet 0 port.
- The Ethernet 0 interface is disabled or misconfigured.
- The system is configured correctly, but the network is down or misconfigured.

Resolution:

Step 1 Verify that the network cable is connected to the Ethernet 0 port, and the Ethernet indicator is lit.

- If the network cable is not connected, connect it.
- If the network cable is connected but the Ethernet indicator is not lit, these are the probable causes:
  - The network cable is faulty.
  - The network cable is the wrong type (for example, a cross-over type, rather than the required straight-through type).
  - The port on the default gateway to which the system connects is down.

If the network cable is connected and the Ethernet indicator is on but the system cannot connect to the network, continue.

Step 2 Use the **ping** command to perform the following tests:

a. Try to ping a well-known host on the network. A DNS server is a good target host.

If the ping command gets a response, the system is connected to the network. If it cannot connect to a particular host, the problem is either with the network configuration or that host. Contact your network administrator for assistance.

If the ping command does not get a response, continue.

b. Attempt to connect to another host on the same subnet as the system.

If the ping command can connect to a host on the same subnet, but cannot connect to a host on a different subnet, the default gateway is probably down.

If the ping command cannot connect to any hosts, continue.

Step 3 Use the **show interfaces** command to determine if the Ethernet 0 interface is disabled or misconfigured. For more information, refer to the "show syslog" section on page C-62.

If the Ethernet 0 interface is disabled, enable it. If it is misconfigured, configure it correctly. For more information, refer to "Configuring the Ethernet Ports" section on page 4-7.

If the interface is enabled and correctly configured, continue.

Step 4 Contact your network administrator to verify that there are no conditions on the network that prevent the system from connecting to the network.

If conditions prevent the system from connecting to the network, have your network administrator correct them.

Step 5 If no conditions are preventing the system from connecting to the network, contact the Cisco Technical Assistance Center (TAC).

Cannot Connect to the VLAN Policy Server Using a Web Browser

Problem: You cannot connect to the system by entering its IP address in a web browser.

Possible causes:

- The system cannot connect to the network.
- HTTP or HTTPS is not enabled.
- If connecting via HTTP, the IP address was not appended with **:1741**.
- The client system is not configured. See the "Configuring the Web Browser" section on page 3-17.

Resolution:

Step 1 Make sure that the system can connect to the network by following the procedure in the "VLAN Policy Server Cannot Connect to the Network" section on page A-2. Attempt to connect the system using a web browser.

If you cannot connect, continue.

Step 2 If you are attempting to connect via HTTP, verify that the IP address is appended with `:1741`.

Step 3 If you are attempting to connect via HTTP, verify that HTTP is enabled. If you are attempting to connect via HTTPS, verify that HTTPS is enabled. For more information, see the "Configuring the Ethernet Ports" section on page 4-7.

Step 4 Verify that the browser is configured correctly, and attempt to connect to the VLAN Policy Server. For more information, see the "Configuring the Web Browser" section on page 3-17. If you cannot connect, continue to step 5.

Step 5 At the system console, or through Telnet, verify that the web server and the tomcat log are running by entering the following:

```
# services status
```

If they are running, go to step 7. If they are not running, continue to step 5.

Step 6 Stop the system services by entering the following:

```
# services stop
```

Step 7 Restart the system services by entering the following:

```
# services start
```

Step 8 Try to connect the system using a web browser.

If you cannot connect, continue to step 9.

Step 9 Reboot the system by entering the **reload** command.

For more information about the **reload** command, refer to the "reload" section on page C-35.

Step 10 If you still cannot connect to the system using a web browser, contact the Cisco Technical Assistance Center (TAC) for assistance.

System Time or Date Is Incorrect

Problem: The system time or date is incorrect.

Possible causes:

- NTP is misconfigured.
- The system clock is set incorrectly.

Resolution:

Refer to the "Setting System Date and Time" section on page 4-6 for information about maintaining the system time and date.

System Cannot Boot from the Hard Drive

Problem: The system cannot boot from the hard drive during a reboot.

Possible causes:

- The disk has a physical error.
- The disk image is corrupted.

Resolution:

If the VLAN Policy Server cannot boot from the hard drive, the hard drive needs to be reimaged. Use the recovery CD to reimage your VLAN Policy Server. For more information, see the "Using the Recovery CD" section on page 4-12.

Cannot Connect to System with Telnet or Telnet Interaction Is Slow

Problem: You cannot connect to the system using Telnet or Telnet interaction, even though the system is connected to the network.

Possible Causes:

- Telnet is disabled or configured incorrectly.
- The VLAN Policy Server cannot recognize hostnames.

Note If you are not using name recognition, slow or nonexistent Telnet interaction is an expected problem. For more information, see the "Name Resolution" section on page 3-15.

Resolution:

If the problem is not in the network, perform the following steps (connect to the console port if you cannot Telnet to the VLAN Policy Server):

Step 1 Check the Telnet settings to be sure Telnet is enabled and configured correctly. For more information, do the following:

- To check the Telnet settings, or to enable or disable Telnet on specific domains or IP addresses, see the "telnetenable" section on page C-69.
- To enable or disable Telnet on individual ports, see the "firewall" section on page C-21.

Step 2 If you have specified hosts in telnetenable, make sure the host from which you are attempting to Telnet is on the list.

Step 3 If you are using a DNS server, perform the following steps:

a. Configure the system to use a functioning DNS server by entering:

```
# ip name-server ip-address
```

where *ip-address* is the IP address of the DNS server.

If you are using the import command-line interface (CLI) command, proceed to Step 4.

b. Verify that the system can get DNS services from the network by entering the following command:

```
# nslookup dns-name {hostname | ip-address}
```

where *dns-name* is the DNS name of a host on the network that is registered in DNS and *hostname,* and *ip-address* is the same IP address specified in Step 2. The command returns the IP address of the host.

c. If the system cannot resolve DNS names to IP addresses, the DNS server it is using is not working properly.

Resolve the network DNS problem, then continue.

Step 4 If you are using the **import** CLI command to resolve hostnames, verify that the VLAN Policy Server can resolve hostnames by entering the following command:

```
ping hostname
```

where *hostname* is a hostname that has been mapped to an IP address, or imported in a host file, using the **import** command.

Step 5 If the system can resolve DNS names to IP addresses but you still cannot connect to the system using Telnet, or if Telnet interaction with the system is extremely slow, contact the Cisco Technical Assistance Center (TAC).

Devices Not Discovered

Problem: The VLAN Policy Server does not discover certain devices.

Possible Causes:

- Community strings are set incorrectly.
- SNMP is not enabled on the device.
- CDP is not enabled on the device.
- SNMP host is not set in LocalDirector.
- Timeout session is too short.
- Retry number is too low.
- Device is not set as a seed.

Resolution:

For information on resolving these problems, see the VLAN Policy Server online help.

To access the online help relevant to these problems:

Step 1 Point a web browser to the VLAN Policy Server and log on.

Step 2 Click Help. A new browser window containing the online help appears.

Step 3 Select Performing Administrative Tasks.

APPENDIX B

Technical Specifications

Table B-1 provides the VLAN Policy Server specifications.

Table B-1 VLAN Policy Server Technical Specifications

Component	Specifications
Serial ports	Two 9-pin connectors
RJ-45 ports	RJ-45 connectors to integrated 10/100 Mbps Ethernet controllers
AC power supply wattage	125 W
AC power supply voltage	100–120/200–240 VAC, 50/60 Hz
System battery	CR2032 3-V lithium coin cell
Height	1.7 in. (4.3 cm)
Width	16.7 in. (42.5 cm)
Depth	22 in. (55 cm)
Weight	23 lb (10 kg) maximum
Operating temperature	50° to 95°F (10° to 35°C)
Storage temperature	–40° to 149°F (–40° to 65°C)
Operating relative humidity	8 to 80% (noncondensing) with a humidity gradation of 10% per hour

Table B-1 VLAN Policy Server Technical Specifications (continued)

Component	Specifications
Storage relative humidity	5 to 95% (noncondensing)
Operating maximum vibration	0.25 G (half-sine wave) at a sweep of 3 to 200 Hz for 15 minutes
Storage maximum vibration	0.5 G at 3 to 200 Hz for 15 minutes
Operating maximum shock	Six consecutively executed shock pulses of 41 G for up to 2 ms in the positive and negative x, y, and z axes (one pulse on each side of the system)
Storage (non-operational) maximum shock	Six consecutively executed shock pulses of 71 G for 2 ms in the positive and negative x, y, and z axes (one pulse on each side of the system)
Operating altitude	–50 to 6500 ft (–16 to 2000 m)
Storage altitude	–50 to 35,000 ft (–16 to 10,600 m)

APPENDIX C

Command Reference

This appendix summarizes the VLAN Policy Server command-line interface (CLI) commands. When you make a configuration change using these commands, the system configuration is updated immediately.

This appendix contains the following sections:

CLI Conventions

The command-line interface (CLI) uses the following conventions:

- The key combination **^c** or **Ctrl-c** means hold down the **Ctrl** key while you press the **c** key.
- A string is defined as a nonquoted set of characters.

Do not confuse the VLAN Policy Server CLI with the IOS CLI. They are similar, but they are not identical.

Command Privileges

Access to CLI commands is controlled by your user account privilege level. Users with privilege level 15 can use all commands. Users with privilege level 0 can use only a subset of the commands. The command descriptions in this appendix are organized by privilege level. For more information about user accounts and privileges, refer to the "Administering User Accounts" section on page 4-3.

Checking Command Syntax

The user interface provides several types of responses to incorrect command entries:

- If you enter a command line that does not contain any valid commands, the system displays `Command not found.`
- If you enter a valid command but omit required options, the system displays `Incomplete command.`
- If you enter a valid command but provide invalid options or parameters, the system displays Invalid input.

In addition, some commands have command-specific error messages that notify you that a command is valid, but that it cannot run correctly.

Command History Feature

The CLI provides a command history feature. To display previously entered commands, press the up arrow key. After pressing the up arrow key, you can press the down arrow key to display the commands in reverse order. To run a command, press the Enter key while the command is displayed on the command line. You can also edit commands before pressing the Enter key.

System Help

You can obtain help using the following methods:

- For a list of all commands and their syntax, enter **help**, then press **Enter**.
- For help on a specific command, type the command name, a space, and a question mark, then press **Enter**, for example, **ntp ?**. The help contains command usage information and syntax.

Command Summary

Table C-1 summarizes all commands available on the VLAN Policy Server. Refer to the full description of commands that you are not familiar with before using them.

Table C-1 Command Summary

Command	Privilege Level	Summary Description	Location of Full Description
auth	15	Enables secure remote authentication.	"auth" section on page C-16
backup	15	Backs up the VLAN Policy Server.	"backup" section on page C-17
backupconfig	15	Sets the configuration for all backup and restore operations.	"backupconfig" section on page C-17
cdp	15	Configures the Cisco Discovery Protocol (CDP).	"cdp" section on page C-18

Table C-1 Command Summary (continued)

Command	Privilege Level	Summary Description	Location of Full Description
clock	15	Sets the VLAN Policy Server date and time.	"clock" section on page C-19
erase config	15[1]	Erases the configuration in Flash memory and reload the device.	"erase config" section on page C-20
exit	0	Logs user off of the VLAN Policy Server.	"exit" section on page C-9
gethostbyname	15	Displays IP address of a known domain name.	"gethostbyname" section on page C-23
fsck	N/A[2]	Checks and repairs the filesystem.	"fsck" section on page C-71
firewall		Implements port filtering on the VLAN Policy Server.	"firewall" section on page C-21
hostname	15	Changes the system hostname.	"hostname" section on page C-23
import	15	Imports host files, or maps IP addresses to hostnames.	"import" section on page C-24
install configure	15	Configures the repository that the VLAN Policy Server uses to install updates.	"install configure" section on page C-25
install list	15	Lists software updates and images currently available on a configured repository.	"install list" section on page C-26
install update	15	Installs software updates and images from a configured repository.	"install update" section on page C-27
interface	15	Configures an Ethernet interface.	"interface" section on page C-28
ip domain-name	15	Defines a default domain name.	"ip domain-name" section on page C-29
ip name-server	15	Specifies the address of up to three name servers for name and address resolution.	"ip name-server" section on page C-30
listbackup	15	Lists all current backups at the configured site.	"listbackup" section on page C-31

Table C-1 Command Summary (continued)

Command	Privilege Level	Summary Description	Location of Full Description
nslookup	15	Translates a DNS name to its IP address or an IP address to its DNS name.	"nslookup" section on page C-32
ntp server	15	Configures the Network Time Protocol (NTP) and allows the system clock to be synchronized by a time server.	"ntp server" section on page C-33
ping	0	Sends ICMP echo_request packets for diagnosing basic network connectivity.	"ping" section on page C-9
reload	15[1]	Reboots the system.	"reload" section on page C-35
reinitdb	15	Reinitializes the database.	"reinitdb" section on page C-35
repository	15	Configures the VLAN Policy Server to be a repository server.	"repository" section on page C-36
repository add	15	Transfers software updates and images from a remote server to the VLAN Policy Server local repository.	"repository add" section on page C-37
repository delete	15	Deletes software updates and images on the VLAN Policy Server local repository.	"repository delete" section on page C-38
repository list	15	Lists software updates and images on the configured local or remote repository.	"repository list" section on page C-39
repository server	15	Starts, stops, or displays the status of the VLAN Policy Server local repository.	"repository server" section on page C-40
restore	15	Restores a backed up configuration.	"restore" section on page C-40
route	15	Adds a route through a gateway device.	"route" section on page C-41
services	15	Lists, starts, or stops management services.	"services" section on page C-42
show anilog	15	Displays the VLAN Policy Server ANI log.	"show anilog" section on page C-44
show auth-cli	15	Displays the type of authentication used for secure CLI access.	"show auth-cli" section on page C-45

Table C-1 Command Summary (continued)

Command	Privilege Level	Summary Description	Location of Full Description
show auth-http	15	Displays the type of authentication used for secure HTTP access.	"show auth-http" section on page C-45
show backupconfig	15	Displays the current backup and restore configuration.	"show backupconfig" section on page C-46
show bootlog	0	Displays the messages logged during the last system boot.	"show bootlog" section on page C-46
show cdp neighbor	15	Displays the VLAN Policy Server nearest neighbor on the network.	"show cdp neighbor" section on page C-48
show cdp run	15	Displays the Cisco Discovery Protocol (CDP) configuration.	"show cdp run" section on page C-48
show clock	0	Displays the system date and time in Coordinated Universal Time (UTC).	"show clock" section on page C-10
show collectorlog	15	Displays the VLAN Policy Server collector log.	"show collectorlog" section on page C-49
show config	15	Displays the system configuration.	"show config" section on page C-50
show daemonslog	15	Displays the VLAN Policy Server daemons log.	"show daemonslog" section on page C-50
show dmgtdlog	15	Displays the VLAN Policy Server daemon manager log.	"show dmgtdlog" section on page C-52
show domain-name	0	Displays the system domain name.	"show domain-name" section on page C-11
show hseaccesslog	15	Displays the VLAN Policy Server web access log.	"show hseaccesslog" section on page C-53
show hseerrorlog	15	Displays the VLAN Policy Server web error log.	"show hseerrorlog" section on page C-54
show hsesslaccesslog	15	Displays the VLAN Policy Server web SSL access log.	"show hsesslaccesslog" section on page C-55
show import	15	Displays imported host files.	"show import" section on page C-55

Table C-1 Command Summary (continued)

Command	Privilege Level	Summary Description	Location of Full Description
show install logs	15	Displays the software updates and images available on the configured repository.	"show install logs" section on page C-56
show interfaces	0	Displays information about the system network interface.	"show interfaces" section on page C-12
show ipchains	15	Displays the IP chains for the selected interface.	"show ipchains" section on page C-57
show hosts	15	Displays the VLAN Policy Server host file.	"show hosts" section on page C-52
show maillog	15	Displays the VLAN Policy Server mail log.	"show maillog" section on page C-57
show process	0	Displays information about processes running on the system.	"show process" section on page C-12
show repository	15	Displays the status or the access log of a configured repository.	"show repository" section on page C-59
show route	15	Displays the routes currently configured.	"show route" section on page C-60
show securitylog	15	Displays the VLAN Policy Server secure log information.	"show securitylog" section on page C-60
show snmp-server	15	Displays the VLAN Policy Server SNMP configuration.	"show snmp-server" section on page C-61
show ssh-version	15	Displays the type of SSH enabled.	"show ssh-version" section on page C-62
show syslog	15	Displays syslog information.	"show syslog" section on page C-62
show tech	15	Displays information necessary for the Cisco Technical Assistance Center (TAC) to assist you.	"show tech" section on page C-64
show telnetenable	15	Displays the VLAN Policy Server Telnet status.	"show telnetenable" section on page C-64

Table C-1 Command Summary (continued)

Command	Privilege Level	Summary Description	Location of Full Description
show tomcatlog	15	Displays the VLAN Policy Server tomcat log.	"show tomcatlog" section on page C-65
show version	0	Displays information about the current software on the system.	"show version" section on page C-13
shutdown	15	Shuts down the system in preparation for powering it off.	"shutdown" section on page C-66
snmp-server	15	Configures an snmp agent.	"snmp-server" section on page C-67
ssh	15	Connects to an external host using SSH.	"ssh" section on page C-68
ssh-version	15	Enables Secure Shell (SSH) 1, SSH 2, or both SSH 1 and SSH 2.	"ssh-version" section on page C-68
telnet	15	Telnets to an external host.	"telnet" section on page C-69
telnetenable	15	Configures Telnet access.	"telnetenable" section on page C-69
traceroute	0	Displays the network route to a specified host and identifies faulty gateways.	"traceroute" section on page C-14
username	15	Creates a new user account or changes an account properties.	"username" section on page C-70

[1] This command is also available in the maintenance image.

[2] This command is available only in the maintenance image.

Command Description Conventions

Command descriptions in this document and in the CLI help system use the following conventions:

- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate optional elements.
- Braces ({ }) indicate a required choice. Braces within square brackets ([{ }]) indicate a required choice within an optional element.

- Boldface indicates commands and keywords that are entered literally as shown.
- Italics indicate arguments for which you supply values.

Privilege Level 0 Commands

This section describes the privilege level 0 commands.

exit

To log off of the system, use the exit command.

exit

Syntax Description

This command has no arguments or keywords.

Example

The following command logs you off of the system:

```
exit
```

ping

To send ICMP echo_request packets for diagnosing basic network connectivity, use the **ping** command.

ping [**-c** *count*] [**-i** *wait*] [**-s** *packetsize*] [**-n**] {*hostname* | *ip-address*}

Syntax Description

c	Sets the number of echo packets to send.
count	Number of echo packets to send.
i	Sets the amount of time to wait between sending each packet.

wait	Amount of time to wait between sending each packet, in seconds. The default is 1.
s	Sets the size of each echo packet.
packetsize	The size of each echo packet, in bytes. The default is 56.
n	Disables reverse DNS lookup.
hostname	Host name of system to ping.
ip-address	IP address of system to ping.

Usage Guidelines

To use this command with the *hostname* argument, DNS must be configured on the system. To force the time-out of a nonresponsive host or to eliminate a loop cycle, press **Ctrl-c**.

Example

This command sends 4 echo packets to the host otherhost with a wait time of 5 seconds between each packet:

```
ping -c 4 -i 5 209.165.200.224

PING 209.165.200.224 (209.165.200.224) from 209.165.201.0 : 56(84)
bytes of data.
64 bytes from dns-sj1.cisco.com (209.165.200.224): icmp_seq=0 ttl=246
time=16.3 ms
64 bytes from dns-sj1.cisco.com (209.165.200.224): icmp_seq=1 ttl=246
time=2.0 ms
64 bytes from dns-sj1.cisco.com (209.165.200.224): icmp_seq=2 ttl=246
time=2.1 ms
64 bytes from dns-sj1.cisco.com (209.165.200.224): icmp_seq=3 ttl=246
time=2.1 ms
```

show clock

To display the system date and time in Coordinated Universal Time (UTC), use the **show clock** command.

show clock

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use the **show clock** command to display the system date and time. For more information about the system time, see the "Setting System Date and Time" section on page 4-6.

Example

This command displays the system date and time:

```
show clock
12:43:47 Jun 20 2001
```

Related Commands

clock

ntp server

show domain-name

To display the system domain name, use the **show domain-name** command.

show domain-name

Syntax Description

This command has no arguments or keywords.

Example

This command displays the system domain name:

```
show domain-name
cisco.com
```

show interfaces

To display information about the system network interface, use the **show interfaces** command.

show interfaces

Syntax Description

This command has no arguments or keywords.

Example

This command displays information about system network interfaces:

```
show interfaces
eth0      Link encap:Ethernet  HWaddr 00:02:B3:35:FD:CC
          inet addr:209.165.200.224 Bcast:209.165.201.0
           Mask:255.255.255.224
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:80309 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22451 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:5 Base address:0xef00 Memory:d0c7e000-d0c7ec40
```

Related Commands

interface

show process

To display information about processes running on the system, use the **show process** command.

show process [**page**]

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.

Example

This command displays information about processes running on the system:

```
show process page
PID  PPID     ELAPSED    SZ                  STARTED TTY  COMMAND
    1     0  4-20:04:35   277 Fri Jun 15 16:54:03 2001 ?    init
    2     1  4-20:04:35     0 Fri Jun 15 16:54:03 2001 ?    kflushd
    3     1  4-20:04:35     0 Fri Jun 15 16:54:03 2001 ?    kupdate
    4     1  4-20:04:35     0 Fri Jun 15 16:54:03 2001 ?    kpiod
    5     1  4-20:04:35     0 Fri Jun 15 16:54:03 2001 ?    kswapd
    6     1  4-20:04:28     0 Fri Jun 15 16:54:10 2001 ?    kreiserfsd
   81     1  4-20:04:25     0 Fri Jun 15 16:54:13 2001 ?    kreiserfsd
   82     1  4-20:04:25     0 Fri Jun 15 16:54:13 2001 ?    kreiserfsd
   83     1  4-20:04:25     0 Fri Jun 15 16:54:13 2001 ?    kreiserfsd
   84     1  4-20:04:25     0 Fri Jun 15 16:54:13 2001 ?    kreiserfsd
   85     1  4-20:04:24     0 Fri Jun 15 16:54:14 2001 ?    kreiserfsd
  199     1  4-20:04:23   290 Fri Jun 15 16:54:15 2001 ?    watchdog
  213     1  4-20:04:23   342 Fri Jun 15 16:54:15 2001 ?    idled
  402     1  4-20:04:17   290 Fri Jun 15 16:54:21 2001 ?    syslogd
  411     1  4-20:04:17   360 Fri Jun 15 16:54:21 2001 ?    klogd
  517     1  4-20:04:15   327 Fri Jun 15 16:54:23 2001 ?    crond
  531     1  4-20:04:15   286 Fri Jun 15 16:54:23 2001 ?    inetd
  540     1  4-20:04:14   585 Fri Jun 15 16:54:24 2001 ?    sshd
  585     1  4-20:04:09   842 Fri Jun 15 16:54:29 2001 ?    dmgtd.lnx
-----------more-----------
```

show version

To display information about the current software on the system, use the **show version** command.

show version

Syntax Description

This command has no arguments or keywords.

Example

This command displays the current software on the system:

```
show version
Copyright (c) 1999-2000 by Cisco Systems, Inc.
Build Version (166) Mon Jun 11 16:56:23 PDT 2001
Uptime: 4 days 20 hours 6 mins
Linux/UID32 version 2.2.16-13bipsec.uid32 (gcc version egcs1
```

traceroute

To display the network route to a specified host and identify faulty gateways, use the **traceroute** command.

traceroute [-f *first_ttl***] [-m** *max_ttl***] [-w** *waittime***]** *host* **[***packetlength***]**

Syntax Description

-f	(Optional) Sets the time-to-live used in the first outgoing probe packet.
first_ttl	Time-to-live value of the first outgoing probe packet. The default is 1 hop.
-m	(Optional) Sets the maximum time-to-live (maximum number of hops) used in outgoing probe packets.
max_ttl	Maximum time-to-live for outgoing probe packets. The default is 30 hops.
-w	(Optional) Sets the time to wait for a response to a probe, in seconds.
waittime	Time to wait for a response to a probe, in seconds. The default is 5.
host	Name or IP address of host to which to connect.
packetlength	(Optional) The length of the packet to send, in bytes. The default and minimum value is 40.

Usage Guidelines

Use the **traceroute** command to trace the network route to a specified host and identify faulty gateways. The command displays a list of the hosts that receive probe packets as they travel to the destination host, in the order that the receiving hosts receive the packets. Asterisks (*) appear as the list entry for hosts that do not respond to probing correctly.

Example

This command displays the network route to the host otherhost with a packet time-to-live value of 2, a wait time of 5 seconds, and 50-byte packets:

```
traceroute -m 20 -w 10 cisco.com 50
traceroute to example.com (209.165.200.224), 20 hops max, 50 byte
packets
 1  ex1.com (209.165.200.225)  0.981 ms  0.919 ms  0.926 ms
 2  ex2.com (209.165.200.254)  1.528 ms  0.747 ms 0.661 ms
 3  ex3.com (209.165.200.255)  0.887 ms  0.770 ms  0.744 ms
 4  ex4.com (209.165.201.0)  0.932 ms  0.789 ms  0.679 ms
 5  ex5.com (209.165.201.1)  1.066 ms  1.052 ms  0.983 ms
 6  ex6.com (209.165.201.30)  1.472 ms  1.247 ms  1.847 ms
 7  ex7.com(209.165.201.31)  1.738 ms  1.424 ms  1.658 ms
 8  ex8.com (209.165.202.128)  3.728 ms  2.429 ms  2.804 ms
 9  ex9.com (209.165.202.129)  6.283 ms  5.499 ms 3.285 ms
10  ex10.com (209.165.202.158)  9.926 ms  73.463 ms  3.895 ms
11  ex11.com (209.165.202.159)  70.967 ms *  47.106 ms
```

Related Commands

ping

Privilege Level 15 Commands

This section describes the privilege level 15 commands. Only users with privilege level 15 can run them.

auth

Use the **auth** command to enable secure remote authentication.

auth {cli | http} {local | tacacs *secret server1* **[***server2***] | radius** *secret server1* **[***server2***] | nt** *domain pdc* **[***bdc***]}**

Syntax Description

cli	Enables authentication using the Command Line Interface (CLI).
http	Enables authentication using Hypertext Transfer Protocol (HTTP).
local	Enables local authentication.
tacacs	Enables authentication using the Terminal Access Controller Access Control System (TACACS).
secret	Shared secret code of server.
server1	IP address or DNS name of server from which authentication will occur.
server2	IP address or DNS name of optional secondary server from which authentication could occur.
radius	Enables authentication using Remote Dial-In User Service (RADIUS).
nt	Enables authentication from an NT domain controller.
domain	NT domain name.
pdc	Name of the Primary Domain Controller (PDC).
bdc	Name of the Backup Domain Controller (BDC).

Example

This command enables secure remote authentication from a remote server, using TACACS.

```
auth http tacacs tr5e43 209.165.200.224
```

backup

Use the **backup** command to back up the VLAN Policy Server.

backup [test]

Syntax Description

test	Tests the configured backup hostname, username, password, and directory.

Usage Guidelines

To backup the VLAN Policy Server, use the **backup** command. To configure the backup location, use the **backupconfig** command.

Example

The following command backs up the VLAN Policy Server:

```
backup
```

Related Commands

backupconfig

listbackup

restore

show backupconfig

backupconfig

Use the **backupconfig** command to set the configuration for all backup and restore operations. To clear the backup and restore configuration information, use the **no backupconfig** command.

backupconfig {*hostname***} {***username***} {***password***} [***directory***]**

no backupconfig

Syntax Description

hostname	Host name or IP address of the host system.
username	Username of host system.
password	Password of the host system.
directory	Path to specific backup directory, if different from user's default directory.

Usage guidelines

To set the configuration for all backup and restore operations, use the **backup** command.

Example

The following command configures the backup and restore operations to host 209.165.200.224, sets the username to user1, and sets the password to pass:

```
backupconfig 209.165.200.224 user1 pass
```

The following command clears all backup and restore configuration information:

```
no backupconfig
```

Related Commands

backup

listbackup

restore

show backupconfig

cdp

Use the **cdp** command to configure the Cisco Discovery Protocol.

cdp {run [*port***] | timer** *seconds* **| holdtime** *seconds***}**

no cdp {run [*port***] | timer | holdtime}**

Syntax Description

run	Start cdp.
port	Ethernet port on which CDP will be enabled. Acceptable values are eth0-15.
timer	Set cdp packets retransmission time.
seconds	Amount of time, in seconds, that the system takes to either transmit the cdp packet information or to hold another system's cdp packet information.
holdtime	Set cdp packet info hold time.

Usage Guidelines

Cisco Discovery Protocol (CDP) is a protocol by which one Cisco device can recognize, and be recognized by, another Cisco device. The run command starts the system sending out signals to the other systems. The timer command sets the amount of time, in seconds, that these signals are sent. The holdtime sets the amount of time a system will recognize another system without receiving a signal. For example, if your system's holdtime is set to 30 seconds, and another system that has already been recognized by yours does not send a signal within that 30 seconds, your system will cease to recognize it. If you are using the **no cdp** command, the timer and holdtime commands set their respective values to the default value.

Example

This command sets the cdp packet's retransmission time at 10 seconds:

```
cdp timer 10
```

This command sets the cdp packet's retransmission to its default time:

```
no cdp timer
```

clock

To set the system date and time, use the **clock** command.

clock {set *hh***:***mm***:***ss month day year***}**

Syntax Description

set	Sets the system clock.
*hh***:***mm***:***ss*	Current time (for example, 13:32:00).
month	Current month. You can enter full month names or abbreviations that include at least the first 3 characters of the month name (for example, jan, feb, mar).
day	Day of the month (for example, 1 to 31).
year	Current year (for example, 2000).

Usage Guidelines

To set the date and time, use the **set** option.

If you configure the system to use Network Time Protocol (NTP), you do not need to set the system clock manually using the **clock** command. When setting the clock, enter the current time in Coordinated Universal Time (UTC).

For more information about the system time, refer to the "Setting System Date and Time" section on page 4-6.

Example

This command sets the date and time:

```
clock set 16:00:00 dec 11 2001

Tue Dec 11 16:00:00 UTC 2001
```

Related Commands

ntp server

show clock

erase config

To erase the configuration in Flash memory and reload the device, use the **erase config** command.

erase config

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command to erase the configuration in Flash memory and reload the device.

When you enter the command, you are prompted for confirmation. Enter **yes** to confirm, or press **Enter** to accept the default response **no**.

Caution When you confirm this command, the system configuration is erased and the system reboots automatically. The system will not operate until you reconfigure it.

When the system reboots, you must reconfigure it with the setup program. For information about using the setup program, refer to Chapter 3, “Installing and Configuring the VLAN Policy Server.”

Example

This command erases the system configuration:

```
erase config
This will erase your configuration, return device t
o factory defaults, and reload the device
Do you want to continue?[no]:yes
```

firewall

To implement port filtering on the VLAN Policy Server, use the **firewall** command.

firewall *eth <0-5>* **[public | private] | [icmp telnet ssh snmp https 1741]**

Syntax Description

eth <0-5>	Port to be configured. Acceptable values are eth0-5.
public	Denies access via ICMP, Telnet, SNMP, and the HTTP 1741 port.
private	Denies no access.
icmp	Denies Internet Control Message Protocol (ICMP) ping messages.
telnet	Denies incoming Telnet connections.
ssh	Denies incoming SSH connections.
snmp	Denies incoming SNMP requests.
https	Denies all connections to the SSL HTTP port.
1741	Denies all connections to the HTTP 1741 port.

Usage Guidelines

Use the firewall command to implement port filtering on the VLAN Policy Server. To configure an Ethernet port for secured public access, use the **public** option. To configure an Ethernet port for local access, through a LAN or VLAN, use the **private** option. To *disable* icmp, Telnet, ssh, snmp, https, or to deny connections to the SSL HTTP port or the HTTP 1741 port, use its corresponding option.

Example

The following is an example of a secure Ethernet port configuration:

- The Ethernet 0 port is connected to the Internet, and is configured to be accessible only through HTTPS by entering the following command:

  ```
  firewall eth0 public ssh 1741
  ```

- The Ethernet 1 port is connected to an internal LAN or VLAN, and is configured to be accessible through any of the supported protocols by entering the following command:

  ```
  firewall eth1 private
  ```

  An on-site user has full access to the VLAN Policy Server, but an external user can access it using a secure connection only.

gethostbyname

Use the gethostbyname command to display the IP address of a known domain name.

gethostbyname *host*

Syntax Description

host	Domain name of host.

Example

This command displays the IP address of example.com:

```
gethostbyname example.com
209.165.200.224
```

hostname

To change the system hostname, use the **hostname** command.

hostname *name*

Syntax Description

name	New hostname for the VLAN Policy Server; the name is case sensitive and may be from 1 to 22 alphanumeric characters.

Example

The following example changes the hostname to sandbox:

```
hostname sandbox
```

import

To import host files, or to map IP addresses to hostnames, use the **import** command.

import {host *hostname ipaddress***} | {hosts** *ftp-host username password path***}**

no import {host *hostname ipaddress***} | {hosts}**

Syntax Description

host	Maps one IP address to a hostname.
hostname	Hostname to map IP address to.
ipaddress	IP address to map Hostname to.
hosts	Imports host files from ftp accessible host.
ftp-host	IP address of ftp accessible host.
username	Username use to access ftp accessible host.
password	Password used to access ftp accessible host.
path	Path to ftp accessible host.

Usage Guidelines

To map a single hostname to an IP address, enter the import command as follows:

import host *hostname ipaddress*

To import host files from an external, ftp-accessible server, enter the import command as follows:

import hosts *ftp-host username password path*

To remove an individual IP address from a host file, use the **no** version of the **import** command as follows:

no import host *hostname ipaddress*

To remove an imported host file, use the **no** version of the **import** command as follows:

no import hosts

Example

This command imports host files from the ftp-accessible server ftpserver_1. Ftpserver_1 has the username admin, the password pass, and the path /ftpserver_1/hosts.

```
import hosts ftpserver_1 admin pass /ftpserver_1/hosts
```

This command deletes the hosts imported in the example above:

```
no import hosts
```

install configure

To define the repository that the VLAN Policy Server uses to install software updates and images, use the **install configure** command.

install configure {URL *URL Value* **| default | save}**

Syntax Description

URL	Sets the URL of the repository.
URL Value	The URL of the repository. The URL should take the form http://host:port/path (the path is not a requirement).
default	Configures the VLAN Policy Server to be its own repository. The URL is http://localhost:9851.
save	Saves the current configuration in the install.ini file.

Usage Guidelines

The **install configure** command defines the repository that the VLAN Policy Server uses. A repository is a remote or local server from which a system can download software updates and images. Only HTTP is supported.

Example

The following command configures the VLAN Policy Server to use http://209.165.200.22, with port 9851, as a repository:

```
install configure URL http://209.165.200.224:9851
```

Related Commands

install update

install list

install list

To list software updates and images currently available on the configured repository, use the **install list** command.

install list [all | full | page | updates]

Syntax Description

all	Displays all software updates and images on a configured repository. This command displays the name, the version, the requirements, the type, and a summary of the software.
full	Displays only the complete images on a configured repository. This command displays the name, the version, the requirements, the type, and a summary of the image.
page	Displays only the names of all software updates and images on a configured repository. All other information is omitted.
updates	Displays only the updates on a configured repository. This command displays the name, the version, the requirements, the type, and a summary of the update.

Usage Guidelines

The **install list** command displays software updates and images currently available on a repository. A repository is a remote or local server from which a system can receive software.

Example

Enter the following command to display a list of all available software updates and images on a configured repository:

```
install list all
Name          Version Requires        Type       Summary
EX-2.0         2.0     URT-2.0         UPDATE    User Registration...
EX-2.0.6       2.0.6   URT-2.0.6       UPDATE    User Registration...
EX-2.0.6j      2.0.6j  URT-2.0.6       UPDATE    User Registration...
EX-2.0.7       2.0.7   URT-2.0.7       UPDATE    User Registration...
EX-2.0.7       2.0.7   URT-2.0.7       UPDATE    User Registration...
EX-2.5         2.5     URT-2.5         UPDATE    User Registration...
```

Related Commands

install configure

install update

install update

To install a software update or image, use the **install update** command.

install update *package name*

Syntax Description

package name	Name of the software update or image to be installed. To see the names of software updates and images available for installation, use the **install list** command. For more information, see the "install list" section on page C-26.

Example

The following command installs the update EX-2.0:

```
install update EX-2.0
```

Related Commands

install configure

install list

interface

To configure an Ethernet interface, use the **interface** command.

interface *eth<0-5>* **{[up | down] |** *ipaddress netmask* **[default-gateway** *address***] [up | down]}**

Syntax Description

eth<0-5>	Name of the interface port to be configured. Acceptable values are eth0-5.
up	Enables the interface (the default). If you include the *ipaddress* parameter and want to enable the interface in the same command, either enter the **up** parameter after *ipaddress* and its required parameters, or do not specify the **up** or **down** parameters (**up** is the default).
down	Disables the interface. If you include the *ipaddress* parameter and want to disable the interface in the same command, enter the **down** parameter after *ipaddress* and its required parameters.
ipaddress	The IP address of the interface.
netmask	The netmask of the interface IP address.
default-gateway	Changes the IP address of the default gateway that connects the VLAN Policy Server to the network.
address	The gateway IP address.

Default

When you enter the **interface** command, the interface that you specify is enabled by default. If you want to disable an enabled interface or leave a disabled interface disabled, you must specify the **down** option.

Usage Guidelines

Use the **interface** command to configure an Ethernet interface.

If you change the IP address or hostname, follow these steps to ensure that applications using the system can connect to it correctly:

Step 1 Stop and restart management services by entering:

```
# services stop

# services start
```

Step 2 Verify that management applications that use the system can still connect to it.

Step 3 Reconnect any applications that cannot connect to it using the system's new IP address or hostname.

Example

This command disables the Ethernet 1 interface:

```
interface eth1 down
```

This command sets the Ethernet 0 IP address, netmask, and gateway IP address:

```
interface eth0 209.165.200.224 255.255.255.224 default-gateway
209.165.201.31 up
```

ip domain-name

To define a default domain name, use the **ip domain-name** command. To remove the default domain name, use the **no** form of the command.

ip domain-name *name*

no ip domain-name *name*

Syntax Description

name	Domain name (for example, cisco.com).

Usage Guidelines

Use this command to define a default domain name.

A default domain name allows the system to resolve any unqualified host names. Any IP hostname that does not contain a domain name will have the configured domain name appended to it. If you are using a DNS server, this appended name is resolved by the DNS server, and then added to the host table.

Example

This command defines the default domain name cisco.com:

```
ip domain-name cisco.com
```

This command removes the default domain name:

```
no ip domain-name
```

Related Commands

ip name-server

ip name-server

To specify the address of up to three name servers for name and address resolution, use the **ip name-server** command. To disable a name server, use the **no** form of the command.

ip name-server *ip-address*

no ip name-server *ip-address*

Syntax Description

ip-address	Name server IP address (maximum of 3).

Usage Guidelines

Use the **ip name-server** command to point the system to a specific DNS server. You may configure up to three servers.

If you attempt to configure a fourth name server, the following error message appears:

```
# Name-server table is full.
```

The system must have a functional DNS server configured to function correctly. If it does not, in most cases it will not correctly process requests from management applications that use it. If the system cannot obtain DNS services from the network, Telnet connections to the system will fail or Telnet interaction with the system will become extremely slow. For more information, refer to the "Cannot Connect to System with Telnet or Telnet Interaction Is Slow" section on page A-6.

Example

This command assigns a name server for the system to use for DNS name to address resolution:

```
ip name-server 209.165.200.224
```

This command disables the name server; the system will not use it for name to address resolution:

```
no ip name-server 209.165.200.224
```

Related Commands

ip domain-name

listbackup

Use the **listbackup** command to list all current backups at the configured site.

listbackup

Syntax Description

This command has no arguments or keywords.

Example

The following command lists all current backups at the configured site:

```
listbackup
ex1_06042001_170640: Hostname: ex1 Date: 06042001  time: 1700
ex1_06052001_124543: Hostname: ex1 Date: 06052001  time: 1243
ex1_06052001_155148: Hostname: ex1 Date: 06052001  time: 1558
ex1_06202001_145704: Hostname: ex1 Date: 06202001  time: 1454
```

Related Commands

backup

backupconfig

restore

show backupconfig

nslookup

To translate a DNS name to its IP address or an IP address to its DNS name, use the **nslookup** command.

nslookup {*dns-name* | *ip-address***}**

Syntax Description

dns-name	DNS name of a host on the network.
ip-address	IP address of a host on the network.

Example

The following command translates the DNS name hostname to its IP address:

```
nslookup hostname
Server: dns.ex1.com
Address: 209.165.200.224

Name:    ex1.com
Address: 209.165.201.0
```

ntp server

To configure the Network Time Protocol (NTP) and allow the system clock to be synchronized by a time server, use the **ntp server** command. To disable this function, use the **no** form of this command.

ntp server *ip-address*

no ntp server *ip-address*

Syntax Description

ip-address	IP address of the NTP time server providing clock synchronization.

Usage Guidelines

Use the **ntp server** command to synchronize the system clock with the specified NTP server. If you configure multiple NTP servers, the system will synchronize with the first working NTP server it finds. There is no limit to the number of NTP servers that you can configure.

The **ntp server** command validates the NTP server that you specify. The possible results are:

- If the server is a valid NTP server, a message similar to the following appears:

  ```
  # 19 Jan 00:43:48 ntpdate[1437]: step time server 209.165.200.224
  offset 999.257304
  ```

- If no NTP server with the name or IP address you specified exists, a message similar to the following appears:

  ```
  # 19 Jan 00:43:40 ntpdate[1431]: no server suitable for
  synchronization found
  ```

  In this case, remove the NTP server by using the **no** form of the command, then configure a valid NTP server.

- If the system time is set to a time later than the time on the NTP server, a message similar to the following appears:

  ```
  # 19 Jan 00:43:58 ntpdate[1265]: Can't adjust the time of day:
  Invalid argument.
  ```

  In this case, the **ntp server** command is entered into the system configuration, but NTP will not function. Follow these steps to remove the command and configure NTP correctly:

Step 1 Remove the **ntp server** command from the configuration by entering the **no** form of the command. For example:

```
no ntp server ip-address
```

where *ip-address* is the IP address of the NTP server.

Step 2 Set the system clock to a time that is behind the time on the NTP server using the **clock set** command. For more information about the clock command, refer to the "clock" section on page C-19.

Step 3 Enter the **ntp server** command again to configure the NTP server on the system. For example:

```
ntp server ip-address
```

Example

This command configures the system to use an NTP server:

```
ntp server 209.165.201.0
```

This command configures the system to stop using the NTP server:

```
no ntp server 209.165.201.0
```

Related Commands

clock

reload

To reboot the system, use the **reload** command.

reload

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use the **reload** command to reboot the system.

You are prompted to verify the reload. Enter **yes** to confirm or **no** to cancel the reload.

Caution All processes running on the system stop when you run the reload command. The VLAN Policy Server will not respond while it is reloading.

Example

This command reboots the system:

```
reload
```

Related Commands

shutdown

reinitdb

To reinitialize the database, use the **reinitdb** command.

reinitdb

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

The **reinitdb** command reinitializes the database. This command erases all information contained within the database.

Example

This command reinitializes the database:

```
reinitdb
```

repository

To configure the VLAN Policy Server to be a repository server, use the **repository** command.

repository source *URL*

Syntax Description

source	Sets the location from which the local repository downloads software updates and images.
URL	The IP address of an external server containing software updates and images.

Usage Guidelines

The **repository** command allows the VLAN Policy Server to be a repository both for itself and for external systems. A repository is a remote or local server from which a system can receive software updates and images.

The **repository** command only configures the VLAN Policy Server to be a repository. To configure the VLAN Policy Server to install software updates and images from this repository, see the "install configure" section on page C-25.

Example

To configure the VLAN Policy Server to be a repository, and to download software updates and images from http:// 209.165.200.224, enter the following command:

```
repository source ftp://209.165.200.224
```

Related Commands

repository add

repository delete

repository list

repository server

repository add

To transfer software updates and images from a remote server to the VLAN Policy Server local repository, use the **repository add** command.

repository add *package*

Syntax Description

package	Name of the software update or image to be transferred.

Usage Guidelines

The **repository add** command transfers software updates and images from a remote server to the VLAN Policy Server local repository. You will be prompted to enter a username and password if they are needed to access the remote server.

Example

To transfer the update EX_2.0 from an update server to the local repository, enter the following command:

```
repository add ex_2.0
```

Related Commands

- **repository**
- **repository delete**
- **repository list**
- **repository server**

repository delete

To delete software updates and images on the VLAN Policy Server local repository, use the **repository delete** command.

repository delete [*package* **| all]**

Syntax Description

package	Name of the software update or image to be deleted.
all	Deletes all software updates and images in the local repository.

Usage Guidelines

The **repository delete** command deletes software updates and images on the VLAN Policy Server local repository. A repository is a remote or local server from which a system can receive software updates and images.

Example

The following command deletes the update EX_2.0 from the local repository:

```
repository delete EX_2.0
```

Related Commands

repository

repository add

repository list

repository server

repository list

To list software updates and images on the configured local or remote repository, use the **repository list** command.

repository list {local | remote} [detail] [page]

Syntax Description

local	Lists software updates and packages on the local repository.
remote	Lists software updates and packages on a remote repository.
detail	Includes details of the software updates and images displayed.
page	Displays the software updates and packages one page at a time.

Example

To list the software updates and images available on the configured local repository, with details and one page at a time, enter the following command:

```
repository list local detail page
```

Related Commands

repository

repository add

repository delete

repository server

repository server

To start, stop, or view the status of the VLAN Policy Server local repository, use the **repository server** command.

repository server [stop | start | status]

Syntax Description

stop	Stops the local repository.
start	Starts the local repository.
status	Displays the status of the local repository.

Usage Guidelines

The **repository server** command starts, stops, or displays the status of the VLAN Policy Server local repository. A repository is a remote or local server from which a system can receive software updates and images.

Example

The following command stops the local repository:

```
repository server stop
```

Related Commands

repository

repository add

repository delete

repository list

restore

Use the **restore** command to restore a backed up configuration of the VLAN Policy Server.

restore *restore name*

Syntax Description

restore name	Name of backup to be used to restore the VLAN Policy Server.

Usage Guidelines

To restore a configuration, use the **restore** command. If you use the **restore** command, all current domains, roles, users, and discovery configuration information will be erased.

Example

The following command will restore a backed up configuration:

```
restore backup1
```

Releated Commands

backup

backupconfig

listbackup

show backupconfig

route

To add a route through a gateway device, use the **route** command. To delete a route, use the **no** version of the command.

route {*network address***} netmask {***network netmask***} gateway {***gateway address***}**

no route {*network address***} netmask {***network netmask***}**

Syntax Description

network address	IP address of the network.
netmask	Sets value of the network netmask.
network netmask	Value of the network netmask.
gateway	Sets the IP address of the router or gateway.
gateway address	IP address of router or gateway.

Example

The following command adds a route:

```
route 209.165.201.0 netmask 255.255.255.224 gateway 209.165.200.224
```

The following command deletes the above route:

```
no route 209.165.201.0 netmask 255.255.255.224
```

services

To list, start, or stop the management services running on the system, use the **services** command.

services [status | start | stop]

Syntax Description

status	Displays the management services status.
start	Starts the management services.
stop	Stops the management services.

Usage Guidelines

Use this command to start, stop, or view status of the management services running on the system.

Management services are the software installed on the system by network management applications. Use this command to stop and restart the management services if the system is not responding correctly to a management application. This should cause the services to reset and function properly again.

Example

This command stops management services:

```
services stop
```

This command starts management services:

```
services start
```

This command shows services status:

```
# services status
Process= HSECollector
        State  = Running but busy flag set
        Pid    = 588
        RC     = 0
        Signo  = 0
        Start  = 06/15/01 16:54:32
        Stop   = Not applicable
        Core   = Not applicable
        Info   = HSECollector started.

        Process= HSEANIServer
        State  = Running but busy flag set
        Pid    = 589
        RC     = 0
        Signo  = 0
        Start  = 06/15/01 16:54:32
-----------more-----------
```

Related Commands

show process

show anilog

To display the VLAN Policy Server ANI log, use the **show anilog** command.

show anilog [page] | include *MatchString1* **[***MatchString2***]**

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the VLAN Policy Server ANI log, one page at a time:

```
show anilog page
/var/adm/CSCOets/log/ani.log
SNMPThrPool: Instantiated ex.lib.snmp.lib.timer.DynamicThreadPool,  mi
n=15, max=48, maxIdleSecs=240
2001/12/20 13:43:12 main ani MESSAGE DBConnection: Created new
Database connecti
on [hashCode = 45981573]
2001/12/20 13:43:38 main ani MESSAGE ServletServiceModule: Moxie
Servlet Engine
is ready to receive requests
2001/12/20 15:43:39 HSEStatusPoll ani MESSAGE DBConnection: Created
new Database
 connection [hashCode = 85057415]
2001/12/20 17:43:39 HSEStatusPoll ani MESSAGE DBConnection: Created
new Database
 connection [hashCode = 396959623]
2001/12/20 19:43:39 HSEStatusPoll ani MESSAGE DBConnection: Created
new Database
--More--
```

show auth-cli

To display the type of authentication used for secure CLI access, use the **show auth-cli** command.

show auth-cli

Syntax Description

This command has no arguments or keywords.

Example

This command and response show that the VLAN Policy Server local authentication is being used for the CLI:

```
show auth-cli
local
```

show auth-http

To display the type of authentication used for secure HTTP access, use the **show auth-http** command.

show auth-http

Syntax Description

This command has no arguments or keywords.

Example

This command and response show that the VLAN Policy Server local authentication is being used for the CLI:

```
show auth-http
local
```

show backupconfig

The **show backupconfig** command displays the current backup and restore configuration.

```
show backupconfig
```

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

To display the current backup and restore configuration, use the **show backupconfig** command. If the backup configuration has not been set, the host and username fields display `NONE`.

Example

The following command displays the current backup and restore configuration:

```
show backupconfig
Hostname: 209.165.201.0
Username: user1
```

Related Commands

backup

backupconfig

listbackup

restore

show bootlog

To display the messages logged during the last system boot, use the **show bootlog** command.

show bootlog [page]

Syntax Description

page	Displays command output one screen at a time. Press the **return** key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.

Example

This command displays the messages logged during the last system boot:

```
show bootlog page
Linux/UID32 version 2.2.16-13bipsec.uid32 (gcc version egcs1
Console: colour VGA+ 80x25
Calibrating delay loop... 1133.77 BogoMIPS
start low memory: 0xc0001000 i386_endbase: 0xc009f000
addresses range:: 0xc0f00000  0xc1000000
start memory: c04f8000 end_memory: d0000000
Memory: 257688k/262144k available (988k kernel code, 416k reserved,
2992k data,)
Dentry hash table entries: 262144 (order 9, 2048k)
Buffer cache hash table entries: 262144 (order 8, 1024k)
Page cache hash table entries: 65536 (order 6, 256k)
vmdump: setting dump_execute() as dump_function_ptr ...
VFS: Diskquotas version dquot_6.4.0 initialized
CPU: Intel Pentium III (Coppermine) stepping 06
Checking 386/387 coupling... OK, FPU using exception 16 error
reporting.
Checking 'hlt' instruction... OK.
POSIX conformance testing by UNIFIX
mtrr: v1.35a (19990819) Richard Gooch (rgooch@atnf.csiro.au)
PCI: PCI BIOS revision 2.10 entry at 0xfda95
PCI: Using configuration type 1
-----------more-----------
```

Related Commands

reload

clock

show cdp neighbor

To display the VLAN Policy Server nearest neighbor on the network, use the **show cdp neighbor** command.

show cdp neighbor

Syntax Description

This command has no arguments or keywords.

Example

This command shows the nearest neighbor on the network.

```
show cdp neighbor
cdp neighbor device: Switch
        device type: cisco WS-C2924-XL
        port: FastEthernet0/12
        address: 209.165.201.0
```

show cdp run

To display the Cisco Discovery Protocol (CDP) configuration, use the **show cdp-run** command.

show cdp run

Syntax Description

This command has no arguments or keywords.

Example

This command displays the CDP configuration:

```
show cdp run
CDP protocol is enabled ...
        broadcasting interval is every 60 seconds.
        time-to-live of cdp packets is 180 seconds.

        CDP is enabled on port eth0.
```

show collectorlog

To display the VLAN Policy Server collector log, use the show collectorlog command.

show collectorlog [page] | include *matchstring1* **[***matchstring2***]**

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the VLAN Policy Server collector log, one page at a time:

```
show collectorlog page
/var/adm/CSCOets/log/collector.log
2001/12/20 13:43:18 main HSECollector MESSAGE CollectorMain: Waiting
for databas
e to be ready
2001/12/20 13:43:21 main HSECollector MESSAGE CollectorMain: Database
is ready
SNMPThrPool: Instantiated ex.lib.snmp.lib.timer.DynamicThreadPool,  mi
n=15, max=48, maxIdleSecs=0
2001/12/20 13:43:29 main HSECollector MESSAGE ServletServiceModule:
Moxie Servle
t Engine is ready to receive requests
2001/12/20 13:43:30 PeriodicSchedulerRun:FaultCleanup HSECollector
MESSAGE Colle
ctorDBUtils: DB.TableCleanupCommand=[VACUUM ]
2001/12/20 13:43:30 PeriodicSchedulerRun:FaultCleanup HSECollector
MESSAGE Colle
ctorDBUtils: DB.TableUpdateStatsCommand=[VACUUM ANALYZE ]
2001/12/21 10:39:52 Moxie Servlet Engine:Pooled Thread:1 HSECollector
MESSAGE Se
rvletContextAdaptor: Collector: init
```

show config

To display the system configuration, use the **show config** command.

show config

Syntax Description

This command has no arguments or keywords.

Example

This command displays the system configuration:

```
show config
hostname ex1
interface ethernet0 209.165.201.0 255.255.255.224 default-gateway
209.165.202.128
interface ethernet1 down
interface ethernet2 down
interface ethernet3 down
interface ethernet4 down
interface ethernet5 down
ip domain-name embu-doc
ip name-server 209.165.202.158
username admin epassword ************* privilege 15
```

show daemonslog

To display the VLAN Policy Server daemons log, use the **show daemonslog** command.

show daemonslog [page] | include *matchstring1* **[***matchstring2***]**

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the VLAN Policy Server collector log, one page at a time:

```
show daemonslog page
/var/adm/CSCOets/log/daemons.log
[dmgrDbg] getenv(PX_DBG)=NULL
[dmgrDbg] getenv(PX_MY_DEBUG)=NULL
[dmgrDbg] getenv(PX_MY_TRACE)=NULL
[dmgrDbg] getenv(PX_DBG_LEVEL)=NULL
[dmgrDbg][Thu Dec 20 13:42:53 2001]##### INFO ##### re-evaluate
DbgLevel=0x0
        ++>>it(1) = 8077978 <HSECollector>
        ++>>it(1) = 8077898 <HSEANIServer>
        ++>>it(1) = 8077428 <PostgreSQL>
        ++>>it(1) = 8077228 <WebServer>
        ++>>it(1) = 8077328 <Tomcat>
        ++>>it(1) = 80770d8 <ExcepReporter>
        ++>>it(1) = 8076fc8 <CDPbrdcast>
        ++>>it(1) = 8076e58 <PerfMon>
#!/bin/sh -v
#!/bin/sh -v

if [ "$NMSROOT" = "" ]; then
        NMSROOT=/opt/CSCOets
        export NMSROOT
fi

cd $NMSROOT
--More--
```

show dmgtdlog

To display the VLAN Policy Server daemon manager log, use the **show dmgtdlog** command.

show dmgtdlog [page] | include *matchstring1* **[***matchstring2***]**

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the VLAN Policy Server collector log, one page at a time:

```
show dmgtdlog page
/var/adm/CSCOets/log/dmgtd.log
Dec 20 13:42:56 ex dmgt[712]: #3001:TYPE=INFO:Using port: tcp/42340.
Dec 20 13:42:56 ex dmgt[714]: #3007:TYPE=INFO:Started application(HSEC
ollector) "/bin/nice -n 19 /opt/CSCOets/bin/collector" pid=715.
Dec 20 13:42:56 ex dmgt[714]: #3007:TYPE=INFO:Started application(HSEA
--More--
```

show hosts

To display your VLAN Policy Server host file, use the **show hosts** command.

show hosts [page]

Syntax Description

page Displays command output one screen at a time.

Example

The following command displays your VLAN Policy Server host file, one page at a time:

```
show hosts page
```

show hseaccesslog

To display the VLAN Policy Server web access log, use the **show hseaccesslog** command.

show hseaccesslog [page] | include *matchstring1* **[***matchstring2***]**

Syntax Description

page Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.

include Filters the command output to display only the records that contain the specified string of characters.

matchstring1 String of characters to search for in the command output.

matchstring2 (Optional) Another string of characters to search for in the command output.

Example

The following command displays the VLAN Policy Server collector log, one page at a time:

```
show hseaccesslog page
/var/adm/CSCOets/log/access_log
209.165.200.224 - - [21/Dec/2001:10:38:54 +0000] "GET / HTTP/1.0" 302
276 "-" "Moz
illa/4.76 [en]C-CCK-MCD   (Windows NT 5.0; U)"
209.165.200.224 - - [21/Dec/2001:10:38:54 +0000] "GET
/perl/login-form.cgi HTTP/1.
```

```
0" 200 2268 "-" "Mozilla/4.76 [en]C-CCK-MCD   (Windows NT 5.0; U)"
209.165.200.224 - - [21/Dec/2001:10:38:55 +0000] "GET /icons/hse.gif
HTTP/1.0" 200
 5554 "http://209.165.201.0:1741/perl/login-form.cgi" "Mozilla/4.76
[en]C-CCK-MC
D   (Windows NT 5.0; U)"
209.165.200.224 - - [21/Dec/2001:10:38:55 +0000] "GET
/icons/left_top.gif HTTP/1.0
" 200 324 "http://209.165.201.0:1741/perl/login-form.cgi"
"Mozilla/4.76 [en]C-CC
K-MCD   (Windows NT 5.0; U)"
--More--
```

show hseerrorlog

To display the VLAN Policy Server Web error log, use the **show hseerrorlog** command.

show hseerrorlog [page] | include *matchstring1* **[***matchstring2***]**

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the VLAN Policy Server collector log, one page at a time:

```
show hseerrorlog page
/var/adm/CSCOets/log/error_log
[Thu Dec 20 13:43:00 2001] [error] (22)Invalid argument: <Perl>:
Invalid command
 'secret', perhaps mis-spelled or defined by a module not included in
the server
```

```
 configuration
[Thu Dec 20 13:43:00 2001] [error] (22)Invalid argument: <Perl>: 
Invalid command
 'line', perhaps mis-spelled or defined by a module not included in 
the server c
onfiguration
[Thu Dec 20 13:43:00 2001] [error] (22)Invalid argument: <Perl>:
```

show hsesslaccesslog

To display the VLAN Policy Server Web SSL log, use the **show hsesslaccesslog** command.

show hsesslaccesslog [page] | include *matchstring1* **[***matchstring2***]**

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the VLAN Policy Server collector log, one page at a time:

```
show hsesslaccesslog page
```

show import

To display an imported host file, use the **show import** command.

show import *hosts*

Syntax Description

hosts	Name of server that host files were imported from.

Example

This command displays the imported host file:

```
show import ftpserver_1
```

show install logs

To display the software updates and images available on the configured repository, use the **show install logs** command.

show install logs [short | long] [page]

Syntax Description

short	Displays only the names of software updates and images on the configured repository.
long	Displays the names and descriptions of software updates and images on the configured repository.
page	Displays command output one screen at a time.

Example

The following command displays the software updates and images available on the configured browser, one screen at a time:

```
show install updates page
2
NAME=EX-2.0a
```

show ipchains

To display the IP chains for the selected interface, use the **show ipchains** command.

show ipchains *eth<0-5>*

Syntax Description

eth<0-5>	Name of the interface port to be configured. Acceptable values are eth0-5.

Example

The following command displays the IP chains for the ethernet 0 interface:

```
show ipchains eth0
Chain ineth0 (1 references):
target     prot opt     source                destination
ports
ACCEPT     tcp  -y--l-  anywhere             ex.help     any ->   telt
ACCEPT     tcp  ------  anywhere             ex.help     any ->   telt
ACCEPT     tcp  ------  anywhere             ex.help     any ->   3345
ACCEPT     tcp  -y--l-  anywhere             ex.help     any ->   ssh
```

show maillog

To display the VLAN Policy Server mail log, use the **show maillog** command.

show maillog [page] | include *matchstring1* **[***matchstring2***]**

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.

matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the VLAN Policy Server collector log, one page at a time:

```
show maillog page
/var/log/maillog
Dec 21 04:02:06 ex sendmail[11643]: EAA11643: from=root, size=307, cla
ss=0, pri=30307, nrcpts=1, msgid=<200112210402.EAA11643@ex.help>, rela
y=root@localhost
Dec 21 04:02:06 ex sendmail[11660]: EAA11643: SYSERR(root): Cannot exe
c /usr/bin/procmail: No such file or directory
Dec 21 04:02:06 ex sendmail[11643]: EAA11643: to=root, ctladdr=root (0
/0), delay=00:00:06, xdelay=00:00:00, mailer=local, stat=Operating
system error
```

show proc

To display the VLAN Policy Server active process statistics, use the **show proc** command.

show proc [page]

Syntax Description

page	Displays command output, one screen at a time.

Example

The following command displays the VLAN Policy Server active process statistics, one page at a time:

```
show proc page
PID     ELAPSED    SZ                  STARTED TTY  COMMAND
    1    22:29:10   277 Thu Dec 20 13:42:29 2001 ?    init
    2    22:29:10     0 Thu Dec 20 13:42:29 2001 ?    kflushd
    3    22:29:10     0 Thu Dec 20 13:42:29 2001 ?    kupdate
    4    22:29:10     0 Thu Dec 20 13:42:29 2001 ?    kpiod
    5    22:29:10     0 Thu Dec 20 13:42:29 2001 ?    kswapd
    6    22:29:03     0 Thu Dec 20 13:42:36 2001 ?    kreiserfsd
   85    22:29:00     0 Thu Dec 20 13:42:39 2001 ?    kreiserfsd
   86    22:29:00     0 Thu Dec 20 13:42:39 2001 ?    kreiserfsd
   87    22:28:59     0 Thu Dec 20 13:42:40 2001 ?    kreiserfsd
   88    22:28:59     0 Thu Dec 20 13:42:40 2001 ?    kreiserfsd
   89    22:28:59     0 Thu Dec 20 13:42:40 2001 ?    kreiserfsd
  208    22:28:57   290 Thu Dec 20 13:42:42 2001 ?    watchdog
  322    22:28:51   342 Thu Dec 20 13:42:48 2001 ?    idled
  510    22:28:51   290 Thu Dec 20 13:42:48 2001 ?    syslogd
  519    22:28:50   361 Thu Dec 20 13:42:49 2001 ?    klogd
  637    22:28:48   327 Thu Dec 20 13:42:51 2001 ?    crond
  651    22:28:48   286 Thu Dec 20 13:42:51 2001 ?    inetd
17076       18:23   364 Fri Dec 21 11:53:16 2001 ?     \_ in.telnetd
17077       18:23   575 Fri Dec 21 11:53:16 2001 0     |   \_ login
-----------more-----------
```

show repository

To display the status or the access log of a configured repository, use the **show repository** command.

show repository {status | access-log} [page]

Syntax Description

status	Displays the status of the local repository.
access-log	Displays the access-log of the local repository.
page	Displays command output one screen at a time.

Example

This command displays the status of the configured repository:

```
show repository status
Repository Source: 171.69.212.146:9851
repository is running.
```

show route

To display the routes currently configured, use the show route command.

show route

Syntax Description

This command has no arguments or keywords.

Example

This command displays the currently configured routes:

```
show route
Destination     Gateway Genmask         Flags Metric Ref    Use Iface
209.165.200.224 0.0.0.0 255.255.255.224 UH    0      0        0 eth0
209.165.200.225 0.0.0.0 255.255.255.224 U     0      0        0 eth0
209.165.200.254 0.0.0.0 255.255.255.224 U     0      0        0 lo
209.165.202.128 0.0.0.0 255.255.255.224 UG    0      0        0 eth0
```

show securitylog

To display the VLAN Policy Server secure log information, use the **show securitylog** command.

show securitylog [page] | include *matchstring1* **[***matchstring2***]**

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the VLAN Policy Server security log, one page at a time:

```
show securitylog page
/var/log/secure
Dec 20 13:45:23 ex in.tftpd[1381]: connect from 209.165.200.224
Dec 20 13:45:27 ex in.tftpd[1383]: connect from 209.165.200.224
Dec 20 13:45:31 ex in.tftpd[1385]: connect from 209.165.200.224
Dec 20 13:45:35 ex in.tftpd[1387]: connect from 209.165.200.224
Dec 20 13:45:39 ex in.tftpd[1389]: connect from 209.165.200.224
Dec 20 13:45:44 ex in.tftpd[1391]: connect from 209.165.200.224
Dec 20 13:45:48 ex in.tftpd[1393]: connect from 209.165.200.224
Dec 20 13:45:52 ex in.tftpd[1395]: connect from 209.165.200.224
Dec 20 13:45:56 ex in.tftpd[1397]: connect from 209.165.200.224
Dec 20 13:46:00 ex in.tftpd[1399]: connect from 209.165.200.224
Dec 20 13:46:04 ex in.tftpd[1412]: connect from 209.165.200.224
Dec 20 13:46:27 ex in.tftpd[1424]: connect from 209.165.200.224
Dec 20 13:46:31 ex in.tftpd[1426]: connect from 209.165.200.224
Dec 20 13:46:35 ex in.tftpd[1428]: connect from 209.165.200.224
Dec 20 13:46:39 ex in.tftpd[1430]: connect from 209.165.200.224
Dec 20 13:46:43 ex in.tftpd[1432]: connect from 209.165.200.224
Dec 20 13:46:47 ex in.tftpd[1434]: connect from 209.165.200.224
--More--
```

show snmp-server

To display the VLAN Policy Server SNMP configuration, use the **show snmp-server** command.

show snmp-server

Syntax Description

This command has no arguments or keywords.

Example

The following command displays the VLAN Policy Server SNMP configuration:

```
show snmp-server
RW community string: private
        RO community string: public

        sysLocation: your site information
        sysContact: your contact information

        trap-forwarding is disabled
```

show ssh-version

To display the type of SSH enabled, use the **ssh-version** command.

show ssh-version

Syntax Description

This command has no arguments or keywords.

Example

This command displays the type of SSH that is enabled:

```
show ssh-version
SSH1, SSH2
```

show syslog

To display syslog information, use the **show syslog** command.

show syslog [page] [include *matchstring1* **[***matchstring2***]]**

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Usage Guidelines

Use this command to display syslog information.

To filter the command output to include only the records that contain the specified string(s) of characters, use the **include** option with one or two character strings to search for. If you include two strings, the command outputs only those records that contain both character strings.

Example

This command displays syslog information:

```
show syslog
Jun 20 16:04:23 ex syslogd 1.3-3: restart.
Jun 20 16:04:23 ex syslog: syslogd startup succeeded
Jun 20 16:04:23 ex kernel: klogd 1.3-3, log source = /proc/kmsg start.
Jun 20 16:04:23 ex kernel: Inspecting /boot/System.map-2.2.16-13bipse2
Jun 20 16:04:23 ex syslog: klogd startup succeeded
-----------more-----------
```

Related Command

interface

show tech

To display information necessary for the Cisco Technical Assistance Center (TAC) to assist you, use the **show tech** command.

show tech [page]

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.

Example

This command displays system information necessary for TAC to assist you.

```
show tech page
/bin/cat: /var/log/secure: Permission denied
Copyright (c) 1999-2000 by Cisco Systems, Inc.
Build Version (166) Mon Jun 11 16:56:23 PDT 2001
Linux/UID32 version 2.2.16-13bipsec.uid32 (gcc version egcs1
Uptime: 0 days 18 hours 35 mins

2 Ethernet interfaces
hostname ex
interface ethernet0 209.165.200.224 255.255.255.224 default-gateway
209.165.202.128
ip name-server 209.165.201.0
username admin epassword ************* privilege 15
eth0      Link encap:Ethernet  HWaddr 00:02:B3:35:FD:CC
          inet addr:209.165.200.224 Bcast:209.165.201.31
Mask:255.255.255.224
-----------more-----------
```

show telnetenable

To display the VLAN Policy Server Telnet status, use the **show telnetenable** command.

show telnetenable

Syntax Description

This command has no arguments or keywords.

Example

The following command shows whether Telnet is enabled or disabled:

```
show telnetenable
telnet enable for: ALL
```

show tomcatlog

To display the VLAN Policy Server Tomcat log, use the **show tomcatlog** command.

show tomcatlog [page] | include *matchstring1* **[***matchstring2***]**

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the VLAN Policy Server tomcat log, one page at a time:

```
show tomcatlog page
/var/adm/CSCOets/log/tomcat.log
2001-12-20 01:43:06 - ContextManager: Adding context Ctx( /examples )
2001-12-20 01:43:06 - ContextManager: Adding context Ctx( /admin )
Starting tomcat. Check logs/tomcat.log for error messages
2001-12-20 01:43:06 - ContextManager: Adding context Ctx(  )
getUIProperties(): unhandled error could be a bad ui.properties
java.lang.NullPointerException
        at java.io.Reader.<init>(Reader.java:68)
        at java.io.InputStreamReader.<init>(InputStreamReader.java:96)
--More--
```

shutdown

To shut down the system in preparation for powering it off, use the **shutdown** command.

shutdown

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command to shut down the VLAN Policy Server in preparation for powering it off. All processes running on the VLAN Policy Server will stop, and it will not respond until you power it off and back on.

You are prompted to verify the shutdown. Enter **yes** to continue, or **no** to cancel the shutdown.

Caution Never power off the system without running the **shutdown** command first. Doing so can destroy data and prevent the system from booting.

Example

This command shuts down the system:

```
shutdown
```

Related Commands

reload

snmp-server

To configure a Simple Network Management Protocol (SNMP) agent, use the **snmp-server** command.

snmp-server {community *community-name* **[RO|RW] | location** *sysLocation-info* **| contact** *sysContact-info***}**

no snmp-server {community *community-name* **| location | contact}**

Syntax Description

community	Sets the community strings that permit access to the SNMP.
community-name	The community name string.
RO	Read only.
RW	Read/write.
location	Sets the system location string.
sysLocation-info	The location string.
contact	Sets the contact string.
sysContact-info	The contact string.

Example

This command sets an SNMP contact string:

```
snmp-server contact Dial System Operator at Beeper # 27345
```

ssh

The connect to an external host, use the **ssh** command.

ssh [*options***]** *host* **[***command***]**

Syntax Description

options	Standard SSH options. For a list of these options, enter the **ssh** command without any arguments.
host	Name or IP address of host to which to connect.
command	Command for the external host to execute.

Example

Enter the following command to connect to an external host using SSH:

```
ssh 209.165.200.224
```

ssh-version

Use the ssh-version command to enable Secure Shell (SSH) 1, SSH 2, or both SSH 1 and SSH 2.

ssh-version {ssh1 | ssh2 | both}

Syntax Description

ssh1	Enables SSH 1.
ssh2	Enables SSH 2.
both	Enables both SSH 1 and SSH2.

Example

This command enables ssh1:

```
ssh-version ssh1
```

telnet

To Telnet to an external host, use the telnet command.

telnet {*hostname* | *IP address***} [***portnumber***]**

Syntax Description

hostname	Hostname of the external device.
IP address	IP address of the external device.
portnumber	Port number of the external device.

Example

Enter the following command to Telnet to port 9851 of a system with the IP address 209.165.200.224:

```
telnet 209.165.200.224 9851
```

telnetenable

To configure Telnet access, use the **telnetenable** command.

telnetenable {enable [*ip-addresses* | *domains***] | disable | status}**

Syntax Description

enable	Enables Telnet access to the system.
ip-addresses	IP addresses of systems allowed Telnet access. If this argument is used, no other machines will be allowed access. Multiple IP addresses are allowed.
domains	Domains of systems allowed Telnet access. If this argument is used, machines with domains other than the specified domains will be denied Telnet access. Multiple domains are allowed.
disable	Disables Telnet access to the system.
status	Displays current access status.

Default

The default is **disable**.

Usage Guidelines

To enable Telnet access to the system for *all* IP source addresses, use the **telnetenable enable** command alone. To enable *specific* IP addresses, use the **telnetenable enable** command followed by the IP addresses.

Example

This command enables Telnet for all IP source addresses:

```
telnetenable enable
```

username

To create a new user account or change an account's properties, use the **username** command. Use the **no** form of the command to remove a user account.

username *name* **password** *password* **[privilege {0 | 15}]**

no username *name*

Syntax Description

name	Name of the user account to create or remove.
password	Specifies a password for the account.
password	The password for the account.
privilege	(Optional) Specifies the account privilege level.
0	Gives the account level 0 privileges. This is the default.
15	Gives the account level 15 privileges.

Usage Guidelines

Use the **username** command to change the properties of a user account. To assign a user CLI privilege level 15, use the **username** command. You cannot assign CLI privilege level 15 through the web interface. Use the **no** form of the command to remove a user account. The default privilege level is 0 if you do not provide the privilege option.

For more information about managing user accounts and privilege levels, refer to the "Administering User Accounts" section on page 4-3.

Example

This command creates a user account named user1 with password password1 and privilege level 15:

```
username user1 password password1 privilege 15
```

This command removes the user account:

```
no username user1
```

Maintenance Image Commands

This section describes the commands that are available when the system is booted from the maintenance image. For more information about the maintenance image, refer to the "Using the Maintenance Image" section on page 4-9.

erase config

This command is identical to the level 15 **erase config** command. For a description, see the "erase config" section on page C-20.

fsck

To check and repair the filesystem, use the fsck command.

fsck

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use the **fsck** command to check and repair the filesystem. The command might prompt you for confirmation before making certain repairs.

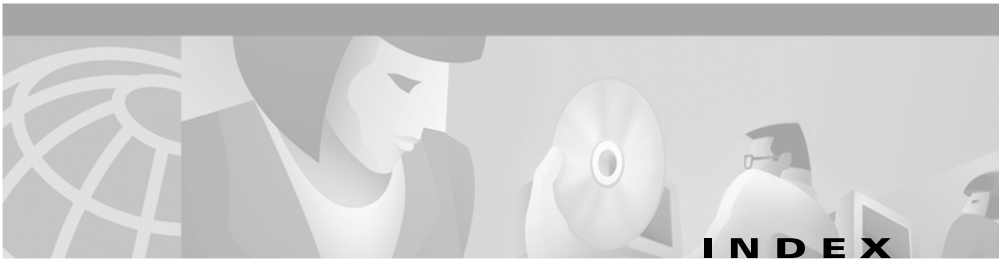
Example

The following command checks and repairs the filesystem:

```
fsck
```

reload

This command is identical to the level 15 **reload** command. For a description, see "reload" section on page C-35.



INDEX