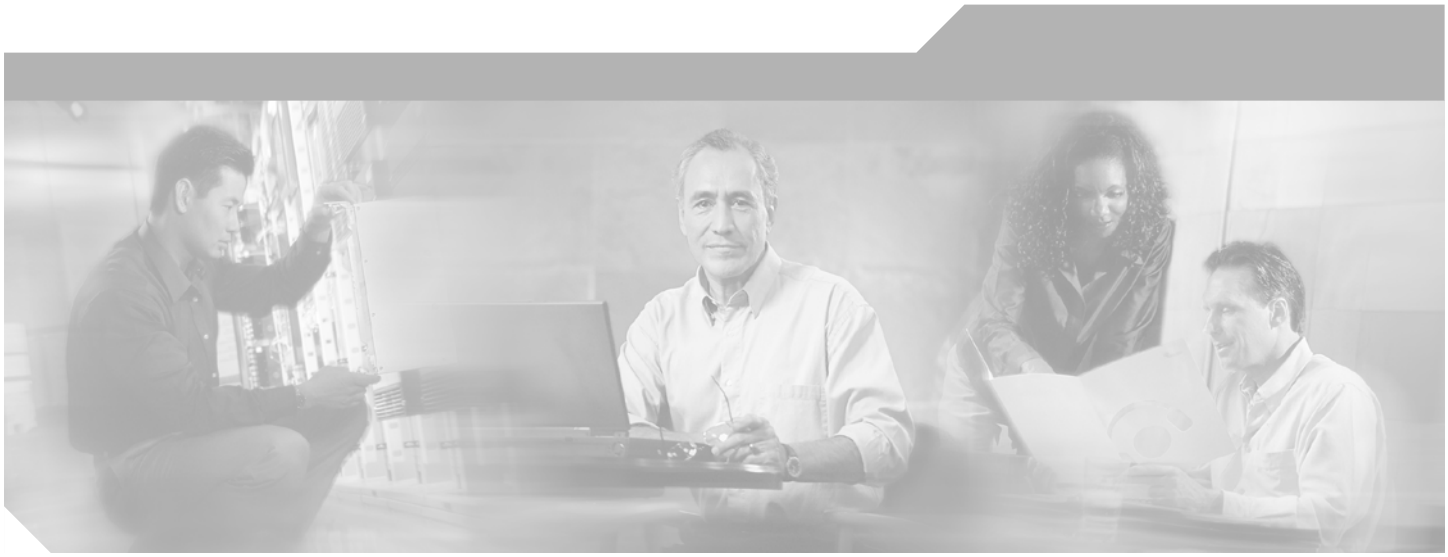


Cisco IOS Configuration Fundamentals and Network Management Command Reference

Release 12.3

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

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 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.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

Cisco IOS Configuration Fundamentals and Network Management Command Reference
Release 12.3
Revision 3 (minor updates): February 1, 2005
Copyright © 2002-2005, Cisco Systems, Inc.
All rights reserved.

CONTENTS

Introduction CFR-1

Configuration Fundamentals and Network Management Commands CFR-22

Appendix

ASCII Character Set and Hexidecimal Values CFR-1122

Introduction

The *Cisco IOS Configuration Fundamentals and Network Management Command Reference* for Release 12.3 provides detailed information about the Cisco IOS command-line interface (CLI) commands used to perform the following tasks:

- Navigate through the CLI by entering, exiting, and using CLI command and configuration modes
- Control terminal operating characteristics
- Configure user menus and banners
- Manage connections and perform basic system management tasks
- Enable the HTTP server and HTTP client on your routing device
- Manipulate files on your routing device using the Cisco IOS File System (IFS)
- Manage configuration files and customize the function of the Cisco IOS software
- Load and copy system images and microcode images
- Maintain router memory
- Modify the rebooting procedures of a router
- Configure basic file transfer services
- Monitor and troubleshoot a router
- Monitor a router and network using Cisco Discovery Protocol (CDP)
- Monitor a router and network Remote Monitoring (RMON)
- Monitor network performance using Cisco Service Assurance Agent (SAA)
- Configure Simple Network Management Protocol (SNMP) on your router
- Configure Cisco Networking Services (CNS)
- Configure the Cisco DistributedDirector
- Configure your router or switch as an XML Subscription Manager (XSM) server

For further information about performing these tasks, refer to the *Cisco IOS Configuration Fundamentals and Network Management Configuration Guide*, which is the companion document for the Command Reference.

Cisco IOS File System Command Syntax

Some commands in this book use URLs as part of the command syntax. URLs used in the Cisco IFS contain two parts: a file system or network prefix, and a file identification suffix. The following tables list URL keywords that can be used in the *source-url* and *destination-url* arguments for all commands in this book. The prefixes listed below can also be used in the *filesystem* arguments in this book.

Table 1 lists common URL network prefixes used to indicate a device on the network.

Table 1 Network Prefixes for Cisco IFS URLs

Prefix	Description
ftp:	Specifies a File Transfer Protocol (FTP) network server.
rcp:	Specifies an remote copy protocol (rcp) network server.
tftp:	Specifies a TFTP server.

Table 2 lists the available suffix options (file indentification suffixes) for the URL prefixes used in Table 1.

Table 2 File ID Suffixes for Cisco IFS URLs

Prefix	Suffix Options
ftp:	[[//[username[:password]@]location]/directory]/filename For example: **ftp://network-config** (*prefix*://*filename*) **ftp://jeanluc:secret@enterprise.cisco.com/ship-confi**g
rcp:	rcp:[[//[username@]location]/directory]/filename
tftp:	tftp:[[//location]/directory]/filename

Table 3 lists common URL prefixes used to indicate memory locations on the system.

Table 3 File System Prefixes for Cisco IFS URLs

Prefix	Description
bootflash:	Bootflash memory.
disk0:	Rotating disk media.
flash: [*partition-number*]	Flash memory. This prefix is available on all platforms. For platforms that do not have a device named **flash:**, the prefix **flash:** is aliased to **slot0:**. Therefore, you can use the prefix **flash:** to refer to the main Flash memory storage area on all platforms
flh:	Flash load helper log files.
null:	Null destination for copies. You can copy a remote file to null to determine its size.
nvram:	NVRAM. This is the default location for the running-configuration file.
slavebootflash:	Internal Flash memory on a slave RSP card of a router configured with Dual RSPs.

Table 3 File System Prefixes for Cisco IFS URLs (continued)

Prefix	Description
slavenvram:	NVRAM on a slave RSP card.
slaveslot0:	First PCMCIA card on a slave RSP card.
slaveslot1:	Second PCMCIA card on a slave RSP card.
slot0:	First PCMCIA Flash memory card.
slot1:	Second PCMCIA Flash memory card.
xmodem:	Obtain the file from a network machine using the Xmodem protocol.
ymodem:	Obtain the file from a network machine using the Ymodem protocol.

For details about the Cisco IFS, and for IFS configuration tasks, refer to the "Configuring the Cisco IOS File System" chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2*.

Flash Memory File System Types

Cisco platforms generally use one of three different Flash memory file system types. Some commands are supported on only one or two file system types. This book notes commands that are not supported on all file system types.

Use Table 4 to determine which Flash memory file system type your platform uses.

Table 4 Flash Memory File System Types

Type	Platforms
Class A	Cisco 7000 family, Cisco 12000 series routers, LightStream1010 switch
Class B	Cisco 1003, Cisco 1004, Cisco 1005, Cisco 2500 series, Cisco 3600 series, and Cisco 4000 series routers, and Cisco AS5200 access servers
Class C	Cisco MC3810 multiservice concentrators, disk0 of Cisco SC3640 System Controllers

Commands by Technology or Task

The *Cisco IOS Configuration Fundamentals and Network Management Configuration Guide* is organized by chapters describing the tasks associated with certain technologies or Cisco IOS features. The following list shows the commands associated with each chapter for your reference.

Part 1: Cisco IOS User Interfaces

Basic Command-Line Interface Commands

- **do**
- **disable**
- **editing**
- **enable**

- **end**
- **exit (EXEC)**
- **exit (global)**
- **full-help**
- **help**
- **history**
- **history size**
- **menu (EXEC)**
- **more <url> begin**
- **more <url> exclude**
- **more <url> include**
- **show <command> append**
- **show <command> begin**
- **show <command> exclude**
- **show <command> include**
- **show <command> redirect**
- **show <command> tee**
- **show history**
- **terminal editing**
- **terminal full-help**
- **terminal history**
- **terminal history size**

SetUp

- **setup**

Terminal Operating Characteristics Commands

- **activation-character**
- **autobaud**
- **buffer-length**
- **databits**
- **data-character-bits**
- **default-value exec-character-bits**
- **default-value special-character-bits**
- **disconnect-character**
- **dispatch-character**
- **dispatch-machine**
- **dispatch-timeout**

- **escape-character**
- **exec-character-bits**
- **hold-character**
- **insecure**
- **length**
- **location**
- **lockable**
- **logout-warning**
- **notify**
- **padding**
- **parity**
- **printer**
- **private**
- **show whoami**
- **special-character-bits**
- **state-machine**
- **stopbits**
- **terminal databits**
- **terminal data-character-bits**
- **terminal dispatch-character**
- **terminal dispatch-timeout**
- **terminal download**
- **terminal escape-character**
- **terminal exec-character-bits**
- **terminal flowcontrol**
- **terminal hold-character**
- **terminal keymap-type**
- **terminal length**
- **terminal monitor**
- **terminal notify**
- **terminal padding**
- **terminal parity**
- **terminal-queue entry-retry-interval**
- **terminal rxspeed**
- **terminal special-character-bits**
- **terminal speed**
- **terminal start-character**
- **terminal stopbits**

- **terminal stop-character**
- **terminal telnet break-on-ip**
- **terminal telnet refuse-negotiations**
- **terminal telnet speed**
- **terminal telnet sync-on-break**
- **terminal telnet transparent**
- **terminal terminal-type**
- **terminal txspeed**
- **terminal-type**
- **terminal width**
- **where**
- **width**

Connection, Menu, and System Banner Commands

- **banner exec**
- **banner incoming**
- **banner login**
- **banner motd**
- **banner slip-ppp**
- **clear tcp**
- **exec**
- **exec-banner**
- **exec-timeout**
- **lock**
- **menu clear-screen**
- **menu command**
- **menu default**
- **menu line-mode**
- **menu options**
- **menu prompt**
- **menu single-space**
- **menu status-line**
- **menu text**
- **menu title**
- **no menu**
- **motd-banner**
- **name-connection**
- **refuse-message**

- **send**
- **service linenumber**
- **vacant-message**

Cisco IOS HTTP Server, Client and Web Browser User Interface Commands

- **international**
- **ip http access-class**
- **ip http authentication**
- **ip http client secure-ciphersuite**
- **ip http client secure-trustpoint**
- **ip http max-connections**
- **ip http path**
- **ip http port**
- **ip http secure-ciphersuite**
- **ip http secure-client-auth**
- **ip http secure-port**
- **ip http secure-server**
- **ip http secure-trustpoint**
- **ip http server**
- **ip http timeout-policy**
- **show ip http server**
- **terminal international**

Part 2: File Management

Cisco IOS File System Commands

- **cd**
- **configure network**
- **copy**
- **delete**
- **dir**
- **erase**
- **erase bootflash**
- **file prompt**
- **format**
- **ip rcmd remote-host**
- **mkdir**
- **more**

- **pwd**
- **rename**
- **rmdir**
- **show file descriptors**
- **show file information**
- **show file systems**
- **squeeze**
- **undelete**
- **verify**
- **write erase**
- **write terminal**

Configuration File Management Commands

- **boot buffersize**
- **boot config**
- **boot host**
- **boot network**
- **clear parser cache**
- **configure terminal**
- **configure memory**
- **configure overwrite-network**
- **parser cache**
- **service compress-config**
- **service config**
- **show configuration**
- **show file**
- **show parser statistics**
- **show running-config**
- **show running-config map-class**
- **show startup-config**

System Image and Microcode Commands

- **copy erase flash**
- **copy verify**
- **copy verify bootflash**
- **copy verify flash**
- **copy xmodem:**
- **copy ymodem:**

- **erase flash:**
- **microcode (7000/7500)**
- **microcode (7200)**
- **microcode (12000)**
- **microcode reload (7000/7500)**
- **microcode reload (7200)**
- **microcode reload (12000)**
- **more flh:logfile**
- **show flh-log**
- **show microcode**
- **xmodem**

Router Memory Commands

- **fsck**
- **memory scan**
- **memory-size iomem**
- **partition**
- **show (Flash file system)**
- **show memory scan**
- **write memory**
- **write network**

Booting Commands

- **boot**
- **boot bootldr**
- **boot bootstrap**
- **boot system**
- **config-register**
- **confreg**
- **continue**
- **reload**
- **show boot**
- **show bootvar**
- **show reload**
- **show version**

Basic File Transfer Services Commands

- **async-bootp**
- **ip ftp passive**
- **ip ftp password**
- **ip ftp source-interface**
- **ip ftp username**
- **ip rarp-server**
- **ip rcmd domain-lookup**
- **ip rcmd rcp-enable**
- **ip rcmd remote-host**
- **ip rcmd remote-username**
- **ip rcmd rsh-enable**
- **ip rcmd source-interface**
- **mop device-code**
- **mop retransmit-timer**
- **mop retries**
- **rsh**
- **show async bootp**
- **tftp-server**
- **tftp-server system**

Part 3: Basic System Management

Basic System Management and Time Services Commands

- **absolute**
- **alias**
- **buffers**
- **buffers huge size**
- **calendar set**
- **clock calendar-valid**
- **clock read-calendar**
- **clock set**
- **clock summer-time**
- **clock timezone**
- **clock update-calendar**
- **downward-compatible-config**
- **hostname**

- **ip bootp server**
- **ip finger**
- **ip telnet source-interface**
- **ip tftp source-interface**
- **load-interval**
- **ntp access-group**
- **ntp authenticate**
- **ntp authentication-key**
- **ntp broadcast**
- **ntp broadcast client**
- **ntp broadcastdelay**
- **ntp clock-period**
- **ntp disable**
- **ntp master**
- **ntp max-associations**
- **ntp multicast**
- **ntp multicast client**
- **ntp peer**
- **ntp refclock**
- **ntp server**
- **ntp source**
- **ntp trusted-key**
- **ntp update-calendar**
- **periodic**
- **prompt**
- **scheduler allocate**
- **scheduler interval**
- **service decimal-tty**
- **service exec-wait**
- **service finger**
- **service hide-telnet-address**
- **service nagle**
- **service prompt config**
- **service tcp-small-servers**
- **service telnet-zero-idle**
- **service udp-small-servers**
- **show aliases**
- **show buffers**

- **show calendar**
- **show clock**
- **show idb**
- **show ntp associations**
- **show ntp status**
- **show registry**
- **show sntp**
- **sntp broadcast client**
- **sntp server**
- **time-range**

General Troubleshooting and System Message Logging Commands

- **attach**
- **clear logging**
- **clear logging xml**
- **diag**
- **exception core-file**
- **exception crashinfo file**
- **exception crashinfo buffersize**
- **exception dump**
- **exception linecard**
- **exception memory**
- **exception protocol**
- **exception region-size**
- **exception spurious-interrupt**
- **execute-on**
- **logging buffered**
- **logging buffered xml**
- **logging console**
- **logging console xml**
- **logging count**
- **logging facility**
- **logging history**
- **logging history size**
- **logging host**
- **logging linecard**
- **logging monitor**
- **logging monitor xml**

- **logging on**
- **logging rate-limit**
- **logging source-interface**
- **logging synchronous**
- **logging trap**
- **ping**
- **ping ip**
- **service sequence-numbers**
- **service slave-log**
- **service tcp-keepalives-in**
- **service tcp-keepalives-out**
- **service timestamps**
- **show c2600 (2600)**
- **show c7200 (7200)**
- **show cls**
- **show context**
- **show controllers (GRP image)**
- **show controllers (line card image)**
- **show controllers logging**
- **show controllers tech-support**
- **show debugging**
- **show environment**
- **show gsr**
- **show gt64010 (7200)**
- **show logging**
- **show logging count**
- **show logging history**
- **show logging xml**
- **show memory**
- **show pci**
- **show pci hardware**
- **show processes**
- **show processes cpu**
- **show processes memory**
- **show protocols**
- **show stacks**
- **show subsys**
- **show tcp**

- **show tcp brief**
- **show tdm connections**
- **show tdm data**
- **show tech-support**
- **show tech-support**
- **test flash**
- **test interfaces**
- **test memory**
- **trace (privileged)**
- **trace (user)**

Part 4: Network Management

SNMP Commands

- **no snmp-server**
- **show management event**
- **show snmp**
- **show snmp engineID**
- **show snmp group**
- **show snmp mib**
- **show snmp mib ifmib ifindex**
- **show snmp mib notification-log**
- **show snmp pending**
- **show snmp sessions**
- **show snmp user**
- **snmp ifmib ifalias long**
- **snmp mib notification-log default**
- **snmp mib notification-log default disable**
- **snmp mib notification-log globalageout**
- **snmp mib notification-log globalsize**
- **snmp mib persist**
- **snmp-server access-policy**
- **snmp-server chassis-id**
- **snmp-server community**
- **snmp-server contact**
- **snmp-server context**
- **snmp-server enable informs**
- **snmp-server enable traps**

- **snmp-server enable traps aaa_server**
- **snmp-server enable traps atm pvc**
- **snmp-server enable traps atm pvc extension**
- **snmp-server enable traps atm pvc extension mibversion**
- **snmp-server enable traps atm subif**
- **snmp-server enable traps bgp**
- **snmp-server enable traps calltracker**
- **snmp-server enable traps dlsw**
- **snmp-server enable traps envmon**
- **snmp-server enable traps frame-relay**
- **snmp-server enable traps frame-relay subif**
- **snmp-server enable traps isdn**
- **snmp-server enable traps mpls ldp**
- **snmp-server enable traps mpls traffic-eng**
- **snmp-server enable traps mpls vpn**
- **snmp-server enable traps pim**
- **snmp-server enable traps pppoe**
- **snmp-server enable traps repeater**
- **snmp-server enable traps rtr**
- **snmp-server enable traps snmp**
- **snmp-server enable traps srp**
- **snmp-server enable traps syslog**
- **snmp-server enable traps voice poor-qov**
- **snmp-server engineID local**
- **snmp-server engineID remote**
- **snmp-server group**
- **snmp-server host**
- **snmp-server informs**
- **snmp-server location**
- **snmp-server manager**
- **snmp-server manager session-timeout**
- **snmp-server packetsize**
- **snmp-server queue-length**
- **snmp-server system-shutdown**
- **snmp-server tftp-server-list**
- **snmp-server trap-authentication**
- **snmp-server trap link**
- **snmp-server trap-source**

- **snmp-server trap-timeout**
- **snmp-server user**
- **snmp-server view**
- **snmp trap link-status**
- **write mib-data**

CDP Commands

- **cdp advertise-v2**
- **cdp enable**
- **cdp holdtime**
- **cdp run**
- **cdp timer**
- **clear cdp counters**
- **clear cdp table**
- **show cdp**
- **show cdp entry**
- **show cdp interface**
- **show cdp neighbors**
- **show cdp traffic**

RMON Commands

- **rmon**
- **rmon alarm**
- **rmon capture-userdata**
- **rmon collection history**
- **rmon collection host**
- **rmon collection matrix**
- **rmon collection rmon1**
- **rmon event**
- **rmon queuesize**
- **show rmon**
- **show rmon alarms**
- **show rmon capture**
- **show rmon events**
- **show rmon filter**
- **show rmon history**
- **show rmon hosts**
- **show rmon matrix**

- **show rmon statistics**
- **show rmon topn**

Service Assurance Agent Commands

- **atm-slm statistics**
- **buckets-of-history-kept**
- **data-pattern**
- **distributions-of-statistics-kept**
- **enhanced-history**
- **filter-for-history**
- **frequency**
- **hops-of-statistics-kept**
- **http-raw-request**
- **hours-of-statistics-kept**
- **lives-of-history-kept**
- **lsr-path**
- **owner**
- **paths-of-statistics-kept**
- **request-data-size**
- **response-data-size**
- **rtr**
- **rtr key-chain**
- **rtr low-memory**
- **rtr reaction-configuration**
- **rtr reaction-trigger**
- **rtr reset**
- **rtr responder**
- **rtr responder type tcpConnect**
- **rtr responder type udpEcho**
- **rtr responder type frame-relay**
- **rtr restart**
- **rtr schedule**
- **rtr slm frame-realy statistics**
- **samples-of-history-kept**
- **show rtr application**
- **show rtr authentication**
- **show rtr collection-statistics**
- **show rtr enhanced-history collection-statistics**

- **show rtr configuration**
- **show rtr distribution-statistics**
- **show rtr enhanced-history distribution-statistics**
- **show rtr history**
- **show rtr operational-state**
- **show rtr reaction-trigger**
- **show rtr responder**
- **show rtr totals-statistics**
- **statistics-distribution-interval**
- **tag**
- **threshold**
- **timeout**
- **tos**
- **type dhcp**
- **type dlsw**
- **type dns**
- **type echo**
- **type frame-relay**
- **type ftp**
- **type http**
- **type jitter**
- **type pathEcho**
- **type pathJitter**
- **type slm controller**
- **type slm interface**
- **type slm atm interface**
- **type slm atm pvc interface**
- **type slm frame-relay interface**
- **type slm frame-realy pvc interface**
- **type tcpConnect**
- **type udpEcho**
- **verify-data**
- **vrfName**

Service Assurance Agent APM Commands

- **clear saa apm cache**
- **saa apm cache-size**
- **saa apm copy**

- **saa apm lowWaterMark**
- **saa apm operation**
- **show saa apm cache**
- **show saa apm information**
- **show saa apm operation**
- **show saa apm results**

Cisco Networking Services Commands

- **clear cns image connections**
- **clear cns image status**
- **cli (cns)**
- **cns config cancel**
- **cns config connect-intf**
- **cns config initial**
- **cns config notify**
- **cns config partial**
- **cns config retrieve**
- **cns connect**
- **cns event**
- **cns id**
- **cns image**
- **cns image password**
- **cns image retrieve**
- **cns image retry**
- **cns inventory**
- **cns mib-access encapsulation**
- **cns notifications encapsulation**
- **cns template connect**
- **config-cli**
- **debug cns image**
- **discover(cns)**
- **line-cli**
- **show cns config status**
- **show cns config connections**
- **show cns config outstanding**
- **show cns config stats**
- **show cns event connections**
- **show cns event gateway**

- **show cns event stats**
- **show cns event status**
- **show cns event subject**
- **show cns image connections**
- **show cns image inventory**
- **show cns image status**
- **template (cns)**

Command Scheduler Commands

- **cli**
- **debug kron**
- **kron occurrence**
- **kron policy-list**
- **policy-list**
- **show kron schedule**

DistributedDirector Commands

- **alias (boomerang)**
- **ip director cache size**
- **ip director cache refresh**
- **ip director cache time**
- **ip director default priorities**
- **ip director default weights**
- **ip director dfp**
- **ip director dfp security**
- **ip director drp rttprobe**
- **ip director drp synchronized**
- **ip director host priority**
- **ip director host weights**
- **ip director server availability**
- **ip director server port availability**
- **ip dns server**
- **ip drp domain**
- **server (boomerang)**
- **show ip director default**
- **show ip director dfp**
- **show ip drp boomerang**
- **snmp-server enable traps director**

- **ttl dns**
- **ttl ip**

VPN Device Manager (VDM) XSM Commands

- **clear xsm**
- **crypto mib topn**
- **show xsm status**
- **show xsm xrd-list**
- **xsm**
- **xsm dvdm**
- **xsm edm**
- **xsm history edm**
- **xsm history vdm**
- **xsm privilege configuration level**
- **xsm privilege monitor level**
- **xsm vdm**

Configuration Fundamentals and Network Management Commands

absolute

To specify an absolute time when a time range is in effect, use the **absolute** command in time-range configuration mode. To remove the time limitation, use the **no** form of this command.

absolute [**start** *time date*] [**end** *time date*]

no absolute

Syntax Description

start *time date*	(Optional) Absolute time and date that the **permit** or **deny** statement of the associated access list starts going into effect. The *time* is expressed in 24-hour notation, in the form of *hours*:*minutes*. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m. The *date* is expressed in the format *day month year*. The minimum start is 00:00 1 January 1993. If no start time and date are specified, the **permit** or **deny** statement is in effect immediately.
end *time date*	(Optional) Absolute time and date that the **permit** or **deny** statement of the associated access list is no longer in effect. Same *time* and *date* format as described for the **start** keyword. The end time and date must be after the start time and date. The maximum end time is 23:59 31 December 2035. If no end time and date are specified, the associated **permit** or **deny** statement is in effect indefinitely.

Defaults

There is no absolute time when the time range is in effect.

Command Modes

Time-range configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.

Usage Guidelines

Time ranges are used by IP and Internetwork Packet Exchange (IPX) extended access lists. For more information on using these functions, see the *Cisco IOS IP Configuration Guide* and the *Cisco IOS AppleTalk and Novell IPX Configuration Guide*. Time ranges are applied to the **permit** or **deny** statements found in these access lists.

The **absolute** command is one way to specify when a time range is in effect. Another way is to specify a periodic length of time with the **periodic** command. Use either of these commands after the **time-range** command, which enables time-range configuration mode and specifies a name for the time range. Only one **absolute** entry is allowed per **time-range** command.

If a **time-range** command has both **absolute** and **periodic** values specified, then the **periodic** items are evaluated only after the **absolute start** time is reached, and are not further evaluated after the **absolute end** time is reached.

Note All time specifications are interpreted as local time. To ensure that the time range entries take effect at the desired times, the software clock should be synchronized using the Network Time Protocol (NTP), or some other authoritative time source. For more information, refer to the "Performing Basic System Management" chapter of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Examples

The following example configures an access list named northeast, which references a time range named xyz. The access list and time range together permit traffic on Ethernet interface 0 starting at noon on January 1, 2001 and going forever.

```
time-range xyz
 absolute start 12:00 1 January 2001
!
ip access-list extended northeast
 permit ip any any time-range xyz
!
interface ethernet 0
 ip access-group northeast in
```

The following example permits UDP traffic until noon on December 31, 2000. After that time, UDP traffic is no longer allowed out Ethernet interface 0.

```
time-range abc
 absolute end 12:00 31 December 2000
!
ip access-list extended northeast
 permit udp any any time-range abc
!
interface ethernet 0
 ip access-group northeast out
```

The following example permits UDP traffic out Ethernet interface 0 on weekends only, from 8:00 a.m. on January 1, 1999 to 6:00 p.m. on December 31, 2001:

```
time-range test
 absolute start 8:00 1 January 1999 end 18:00 31 December 2001
 periodic weekends 00:00 to 23:59
!
ip access-list extended northeast
 permit udp any any time-range test
!
interface ethernet 0
 ip access-group northeast out
```

Related Commands

Command	Description
deny	Sets conditions under which a packet does not pass a named access list.
periodic	Specifies a recurring (weekly) start and end time for a time range.
permit	Sets conditions under which a packet passes a named access list.
time-range	Enables time-range configuration mode and names a time range definition.

activation-character

To define the character you enter at a vacant terminal to begin a terminal session, use the **activation-character** command in line configuration mode. To make any character activate a terminal, use the **no** form of this command.

activation-character *ascii-number*

no activation-character

Syntax Description

ascii-number	Decimal representation of the activation character.

Defaults

Return (decimal 13)

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

See the "ASCII Character Set and Hex Values" appendix for a list of ASCII characters.

Note If you are using the **autoselect** function, set the activation character to the default, Return, and exec-character-bits to 7. If you change these defaults, the application will not recognize the activation request.

Examples

The following example sets the activation character for the console to Delete, which is decimal character 127:

```
Router(config)# line console
Router(config-line)# activation-character 127
```

alias

To create a command alias, use the **alias** command in global configuration mode. To delete all aliases in a command mode or to delete a specific alias, and to revert to the original command syntax, use the **no** form of this command.

alias *mode command-alias original-command*

no alias *mode* [*command-alias*]

Syntax Description

mode	Command mode of the original and alias commands.
command-alias	Command alias.
original-command	Original command syntax.

Defaults

A set of six basic EXEC mode aliases are enabled by default. See the "Usage Guidelines" section of this command for a list of default aliases.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

You can use simple words or abbreviations as command aliases.

Table 5 lists the basic EXEC mode aliases that are enabled by default.

Table 5 Default Command Aliases

Command Alias	Original Command
h	**help**
lo	**logout**
p	**ping**
r	**resume**
s	**show**
w	**where**

The default aliases in Table 5 are predefined. These default aliases can be disabled with the **no alias exec** command.

Common keyword aliases (which cannot be disabled) include **running-config** (keyword alias for **system:running-config**) and **startup-config** (keyword alias for **nvram:startup-config**). See the description of the **copy** command for more information about these keyword aliases.

Note that aliases can be configured for keywords instead of entire commands. You can create, for example, an alias for the first part of any command and still enter the additional keywords and arguments as normal.

To determine the value for the mode argument, enter the command mode in which you would issue the original command (and in which you will issue the alias) and enter the **?** command. The name of the command mode should appear at the top of the list of commands. For example, the second line in the following sample output shows the name of the command mode as "Interface configuration":

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface e0
Router(config-if)# ?
Interface configuration commands:
  access-expression       Build a bridge boolean access expression
 .
 .
 .
```

To match the name of the command mode to the acceptable mode keyword for the **alias** command, issue the **alias ?** command. As shown in the following sample output, the keyword needed to create a command alias for the access-expression command is **interface**:

```
Router(config)# alias ?
  accept-dialin          VPDN group accept dialin configuration mode
  accept-dialout         VPDN group accept dialout configuration mode
  address-family         Address Family configuration mode
  call-discriminator     Call Discriminator Configuration
  cascustom              Cas custom configuration mode
  clid-group             CLID group configuration mode
  configure              Global configuration mode
  congestion             Frame Relay congestion configuration mode
  controller             Controller configuration mode
  cptone-set             custom call progress tone configuration mode
  customer-profile       customer profile configuration mode
  dhcp                   DHCP pool configuration mode
  dnis-group             DNIS group configuration mode
  exec                   Exec mode
  flow-cache             Flow aggregation cache config mode
  fr-fr                  FR/FR connection configuration mode
  interface              Interface configuration mode
 .
 .
 .
Router(config)# alias interface express access-expression
```

For a list of command modes with descriptions and references to related documentation, refer to the "Cisco IOS Command Modes" appendix of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

When you use online help, command aliases are indicated by an asterisk (*), and displayed in the following format:

**command-alias=original-command*

For example, the **lo** command alias is shown here along with other EXEC mode commands that start with "lo":

```
Router# lo?
*lo=logout  lock  login  logout
```

When you use online help, aliases that contain multiple keyword elements separated by spaces are displayed in quotes, as shown here:

```
Router(config)#alias exec device-mail telnet device.cisco.com 25
Router(config)#end
Router#device-mail?
*device-mail=″telnet device.cisco.com 25"
```

To list only commands and omit aliases, begin your input line with a space. In the following example, the alias **td** is not shown, because there is a space before the **t?** command line.

```
Router(config)#alias exec td telnet device
Router(config)#end
Router# t?
telnet terminal test tn3270 trace
```

To circumvent command aliases, use a space before entering the command. In the following example, the command alias **express** is not recognized because a space is used before the command.

```
Router(config-if)#exp?
*express=access-expression
Router(config-if)# express ?
% Unrecognized command
```

As with commands, you can use online help to display the arguments and keywords that can follow a command alias. In the following example, the alias **td** is created to represent the command **telnet device**. The /debug and /line switches can be added to **telnet device** to modify the command:

```
Router(config)#alias exec td telnet device
Router(config)#end
Router#td ?
      /debug     Enable telnet debugging mode
      /line      Enable telnet line mode
      ...
      whois      Whois port
      <cr>
Router# telnet device
```

You must enter the complete syntax for the command alias. Partial syntax for aliases is not accepted. In the following example, the parser does not recognize the command **t** as indicating the alias **td**:

```
Router# t
% Ambiguous command: "t"
```

Examples

In the following example, the alias **fixmyrt** is configured for the **clear iproute 192.168.116.16** EXEC mode command:

```
Router(config)#alias exec fixmyrt clear ip route 192.168.116.16
```

In the following example, the alias **express** is configured for the first part of the **access-expression** interface configuration command:

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface e0
Router(config-if)#?
Interface configuration commands:
  access-expression        Build a bridge boolean access expression
  .
  .
  .
```

```
Router(config-if)#exit
Router(config)#alias ?
  accept-dialin         VPDN group accept dialin configuration mode
  accept-dialout        VPDN group accept dialout configuration mode
  address-family        Address Family configuration mode
  call-discriminator    Call Discriminator Configuration
  cascustom             Cas custom configuration mode
  clid-group            CLID group configuration mode
  configure             Global configuration mode
  congestion            Frame Relay congestion configuration mode
  controller            Controller configuration mode
  cptone-set            custom call progress tone configuration mode
  customer-profile      customer profile configuration mode
  dhcp                  DHCP pool configuration mode
  dnis-group            DNIS group configuration mode
  exec                  Exec mode
  flow-cache            Flow aggregation cache config mode
  fr-fr                 FR/FR connection configuration mode
  interface             Interface configuration mode
 .
 .
 .

Router(config)#alias interface express access-expression
Router(config)#int e0
Router(config-if)#exp?
*express=access-expression

Router(config-if)#express ?
  input   Filter input packets
  output   Filter output packets

!Note that the true form of the command/keyword alias appears on the screen after issuing
!the express ? command.
Router(config-if)#access-expression ?
  input   Filter input packets
  output  Filter output packets
Router(config-if)#ex?
*express=access-expression  exit

!Note that in the following line, a space is used before the ex? command
!so the alias is not displayed.
Router(config-if)# ex?
exit

!Note that in the following line, the alias cannot be recognized because
!a space is used before the command.
Router#(config-if)# express ?
% Unrecognized command

Router(config-if)# end
Router# show alias interface
Interface configuration mode aliases:
  express               access-expression
```

Related Commands

Command	Description
show aliases	Displays command aliases.

alias (boomerang)

To configure an alias name for a specified domain, use the **alias** command in boomerang configuration mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

alias *alias-name*

no alias *alias-name*

Syntax Description

alias-name	Alias name for a specified domain.

Defaults

No domain name alias is configured.

Command Modes

Boomerang configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

The **alias** command can be used only on a Director Response Protocol (DRP) agent. The boomerang client is the DRP agent.

Use the **alias** command to specify one or more alias names for an existing domain. Because the boomerang client maintains separate counters for requests received for each domain name (alias or otherwise), use the **show ip drp boomerang** command to view these counters for a specified domain name and each of its aliases.

Examples

In the following example, the domain name alias is configured for www.boom1.com. The new alias for www.boom1.com is www.boom2.com:

```
Router(config)#  ip drp domain www.boom1.com
Router(config-boomerang)# alias www.boom2.com

Router# show running-config
.
.
.
ip drp domain www.boom1.com
alias www.boom2.com
```

Related Commands

Command	Description
ip drp domain	Adds a new domain to the DistributedDirector client or configures an existing domain and puts the client in boomerang configuration mode.
server (boomerang)	Configures the server address for a specified boomerang domain.
show ip drp	Displays DRP statistics on DistributedDirector or a DRP server agent.
show ip drp boomerang	Displays boomerang information on the DRP agent.
ttl dns	Configures the number of seconds for which an answer received from the boomerang client will be cached by the DNS client.
ttl ip	Configures the IP TTL value for the boomerang response packets sent from the boomerang client to the DNS client in number of hops.

announce config

To specify that an unsolicited configuration inventory is sent out by the CNS inventory agent at bootup, use the **announce config** command in CNS inventory configuration mode. To disable the sending of the configuration inventory, use the **no** form of this command.

announce config

no announce config

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

CNS inventory configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use this command to limit inventory requests by the CNS inventory agent. When configured, the routing device details will be announced on the CNS Event Bus, but the routing device will not respond to any queries from the CNS Event Bus.

Examples

The following example shows how to configure the CNS inventory agent to send out an unsolicited configuration inventory one time only at bootup:

```
Router(config)# cns inventory
Router(cns_inv)# announce config
```

Related Commands

Command	Description
cns inventory	Enables the CNS inventory agent and enters CNS inventory configuration mode.

async-bootp

To configure extended BOOTP requests for asynchronous interfaces as defined in RFC 1084, use the **async-bootp** command in global configuration mode. To restore the default, use the **no** form of this command.

async-bootp *tag* [**:***hostname*] *data*

no async-bootp

Syntax Description

tag	Item being requested; expressed as filename, integer, or IP dotted decimal address. See Table 6 for possible keywords.
:*hostname*	(Optional) This entry applies only to the specified host. The **:***hostname* argument accepts both an IP address and a logical host name.
data	List of IP addresses entered in dotted decimal notation or as logical host names, a number, or a quoted string.

Table 6 tag Keyword Options

Keyword	Description
bootfile	Specifies use of a server boot file from which to download the boot program. Use the optional :*hostname* argument and the *data* argument to specify the filename.
subnet-mask *mask*	Dotted decimal address specifying the network and local subnetwork mask (as defined by RFC 950).
time-offset *offset*	Signed 32-bit integer specifying the time offset of the local subnetwork in seconds from Coordinated Universal Time (UTC).
gateway *address*	Dotted decimal address specifying the IP addresses of gateways for this subnetwork. A preferred gateway should be listed first.
time-server *address*	Dotted decimal address specifying the IP address of time servers (as defined by RFC 868).
IEN116-server *address*	Dotted decimal address specifying the IP address of name servers (as defined by IEN 116).
nbns-server *address*	Dotted decimal address specifying the IP address of Windows NT servers.
DNS-server *address*	Dotted decimal address specifying the IP address of domain name servers (as defined by RFC 1034).
log-server *address*	Dotted decimal address specifying the IP address of an MIT-LCS UDP log server.
quote-server *address*	Dotted decimal address specifying the IP address of Quote of the Day servers (as defined in RFC 865).
lpr-server *address*	Dotted decimal address specifying the IP address of Berkeley UNIX Version 4 BSD servers.
impress-server *address*	Dotted decimal address specifying the IP address of Impress network image servers.

Table 6 tag Keyword Options (continued)

Keyword	Description
rlp-server *address*	Dotted decimal address specifying the IP address of Resource Location Protocol (RLP) servers (as defined in RFC 887).
hostname *name*	The name of the client, which may or may not be domain qualified, depending upon the site.
bootfile-size *value*	A two-octet value specifying the number of 512-octet (byte) blocks in the default boot file.

Defaults

If no extended BOOTP commands are entered, the Cisco IOS software generates a gateway and subnet mask appropriate for the local network.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use the **show async-bootp** EXEC command to list the configured parameters. Use the **no async-bootp** command to clear the list.

Examples

The following example illustrates how to specify different boot files: one for a PC, and one for a Macintosh. With this configuration, a BOOTP request from the host on 172.30.1.1 results in a reply listing the boot filename as pcboot. A BOOTP request from the host named "mac" results in a reply listing the boot filename as "macboot."

```
async-bootp bootfile :172.30.1.1 "pcboot"
async-bootp bootfile :mac "macboot"
```

The following example specifies a subnet mask of 255.255.0.0:

```
async-bootp subnet-mask 255.255.0.0
```

The following example specifies a negative time offset of the local subnetwork of 3600 seconds:

```
async-bootp time-offset -3600
```

The following example specifies the IP address of a time server:

```
async-bootp time-server 172.16.1.1
```

Related Commands

Command	Description
show async bootp	Displays the extended BOOTP request parameters that have been configured for asynchronous interfaces.

atm-slm statistics

To enable the Service Assurance Agent (SAA) ATM Service Level Monitoring (SLM) feature, use the **atm-slm statistics** command in global configuration mode. To disable ATM SLM, use the **no** form of this command.

atm-slm statistics

no atm-slm statistics

Syntax Description

This command has no arguments or keywords.

Defaults

ATM Service Level Monitoring is disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

To generate and retrieve performance statistics for ATM services using SAA, the ATM SLM feature must first be enabled on the device using the **atm-slm statistics** global configuration command. (Note that these performance statistics can be retrieved by other applications such as CNS or Visual Uptime.) If this command is not used, SAA SLM operations (**type slm atm pvc**, **type slm atm interface**, or **type slm controller**) cannot be configured on the system.

Disabling the ATM SLM feature with the **no atm-slm statistics** command will cause any currently configured SAA SLM operations to be removed from the configuration. When ATM SLM is disabled, no CNS/XML requests are processed.

Examples

In the following example, the ATM SLM feature is enabled before an SAA SLM operation is configured for ATM interface 0/1:

```
Router(config)# atm-slm statistics
Router(config)# rtr 1
Router(config-rtr)# type slm atm interface ATM0/1
Router(config-rtr-slm)# enhanced-history interval 900 buckets 100
Router(config-rtr-slm)# exit
Router(config)# rtr schedule 1 start-time now life forever
```

Related Commands

Command	Description
type slm atm pvc	Specifies that the operation is an SAA SLM ATM Circuit operation.

Command	Description
type slm atm interface	Specifies that the operation is an SAA SLM ATM Interface operation.
type slm controller	Specifies that the operation is an SAA SLM ATM or Frame Relay Controller operation.

attach

To connect to a specific line card for the purpose of executing monitoring and maintenance commands on that line card only, use the **attach** command in privileged EXEC mode. To exit from the Cisco IOS software image on the line card and return to the Cisco IOS image on the giabit route processor (GRP), use the **exit** command.

attach *slot-number*

Syntax Description

slot-number	Slot number of the line card you want to connect to. Slot numbers range from 0 to 11 for the Cisco 12012 router and 0 to 7 for the Cisco 12008 router. If the slot number is omitted, you are prompted for the slot number.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2 GS	This command was introduced for the Cisco 12000 series.

Usage Guidelines

You must first use the **attach** privileged EXEC command to access the Cisco IOS software image on a line card before using line card-specific **show** EXEC commands. Alternatively, you can use the **execute-on** privileged EXEC command to execute a **show** command on a specific line card.

After you connect to the Cisco IOS image on the line card using the **attach** command, the prompt changes to `LC-Slotx#`, where *x* is the slot number of the line card.

The commands executed on the line card use the Cisco IOS image on that line card.

You can also use the **execute-on slot** privileged EXEC command to execute commands on one or all line cards.

Note Do not execute the **config** EXEC command from the Cisco IOS software image on the line card.

Examples

In the following example, the user connects to the Cisco IOS image running on the line card in slot 9, gets a list of valid **show** commands, and returns the Cisco IOS image running on the GRP:

```
Router# attach 9

Entering Console for 4 Port Packet Over SONET OC-3c/STM-1 in Slot: 9
Type exit to end this session

Press RETURN to get started!

LC-Slot9# show ?
```

```
  cef       Cisco Express Forwarding
  clock     Display the system clock
  context   Show context information about recent crash(s)
  history   Display the session command history
  hosts     IP domain-name, lookup style, nameservers, and host table
  ipc       Interprocess communications commands
  location  Display the system location
  sessions  Information about Telnet connections
  terminal  Display terminal configuration parameters
  users     Display information about terminal lines
  version   System hardware and software status

LC-Slot9# exit

Disconnecting from slot 9.
Connection Duration: 00:01:04
Router#
```

Note Because not all statistics are maintained on the line cards, the output from some of the **show** commands might not be consistent.

Related Commands

Command	Description
attach shelf	Connects you to a specific (managed) shelf for the purpose of remotely executing commands on that shelf only.
execute-on slot	Executes commands remotely on a specific line card, or on all line cards simultaneously.

autobaud

To set the line for automatic baud rate detection (autobaud), use the **autobaud** command in line configuration mode. To disable automatic baud detection, use the **no** form of this command.

autobaud

no autobaud

Syntax Description

This command has no arguments or keywords.

Defaults

Autobaud detection is disabled. Fixed speed of 9600 bps.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The autobaud detection supports a range from 300 to 19200 baud. A line set for autobaud cannot be used for outgoing connections, nor can you set autobaud capability on a line using 19200 baud when the parity bit is set (because of hardware limitations).

Note Automatic baud rate detection must be disabled by using the **no autobaud** command prior to entering the **rxspeed**, **speed**, or **txspeed** commands.

Examples

In the following example, the auxiliary port is configured for autobaud detection:

```
Router(config)# line aux
Router(config-line)# autobaud
```

banner exec

To specify and enable a message to be displayed when an EXEC process is created (an EXEC banner), use the **banner exec** command in global configuration mode. To delete the existing EXEC banner, use the **no** form of this command.

banner exec *d message d*

no banner exec

Syntax Description

d	Delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the banner message.
message	Message text. You can include tokens in the form $(*token*) in the message text. Tokens will be replaced with the corresponding configuration variable. Tokens are described in Table 7.

Defaults

Disabled (no EXEC banner is displayed).

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.3(7.5)AA	Token functionality was introduced.
12.0(3)T	Token functionality was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

This command specifies a message to be displayed when an EXEC process is created (a line is activated, or an incoming connection is made to a vty). Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

When a user connects to a router, the message-of-the-day (MOTD) banner appears first, followed by the login banner and prompts. After the user logs in to the router, the EXEC banner or incoming banner will be displayed, depending on the type of connection. For a reverse Telnet login, the incoming banner will be displayed. For all other connections, the router will display the EXEC banner.

To disable the EXEC banner on a particular line or lines, use the **no exec-banner** line configuration command.

To customize the banner, use tokens in the form $(*token*) in the message text. Tokens will display current Cisco IOS configuration variables, such as the router's host name and IP address. The tokens are described in Table 7.

Table 7 banner exec Tokens

Token	Information Displayed in the Banner
$(hostname)	Displays the host name for the router.
$(domain)	Displays the domain name for the router.
$(line)	Displays the vty or tty (asynchronous) line number.
$(line-desc)	Displays the description attached to the line.

Examples

The following example sets an EXEC banner that uses tokens. The percent sign (%) is used as a delimiting character. Notice that the $(*token*) syntax is replaced by the corresponding configuration variable.

```
Router(config)# banner exec %
Enter TEXT message.  End with the character '%'.
Session activated on line $(line), $(line-desc). Enter commands at the prompt.
%
```

When a user logs on to the system, the following output is displayed:

```
User Access Verification

Username: joeuser
Password: <password>

 Session activated on line 50, vty default line. Enter commands at the prompt.

Router>
```

Related Commands

Command	Description
banner incoming	Defines a customized banner to be displayed when there is an incoming connection to a terminal line from a host on the network.
banner login	Defines a customized banner to be displayed before the username and password login prompts.
banner motd	Defines a customized message-of-the-day banner.
banner slip-ppp	Defines a customized banner to be displayed when a serial-line IP or point-to-point connection is made.
exec-banner	Controls (enables or disables) the display of EXEC banners and message-of-the-day banners on a specified line or lines.

banner incoming

To define and enable a banner to be displayed when there is an incoming connection to a terminal line from a host on the network, use the **banner incoming** command in global configuration mode. To delete the incoming connection banner, use the **no** form of this command.

banner incoming *d message d*

no banner incoming

Syntax Description

d	Delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the banner message.
message	Message text. You can include tokens in the form $(*token*) in the message text. Tokens will be replaced with the corresponding configuration variable. Tokens are described in Table 8.

Defaults

Disabled (no incoming banner is displayed).

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.3(7.5)AA	Token functionality was introduced.
12.0(3)T	Token functionality was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

Follow the **banner incoming** command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

An *incoming connection* is one initiated from the network side of the router. Incoming connections are also called reverse Telnet sessions. These sessions can display MOTD banners and incoming banners, but they do not display EXEC banners. Use the **no motd-banner** line configuration command to disable the MOTD banner for reverse Telnet sessions on asynchronous lines.

When a user connects to the router, the message-of-the-day (MOTD) banner (if configured) appears first, before the login prompt. After the user successfully logs in to the router, the EXEC banner or incoming banner will be displayed, depending on the type of connection. For a reverse Telnet login, the incoming banner will be displayed. For all other connections, the router will display the EXEC banner.

Incoming banners cannot be suppressed. If you do not want the incoming banner to appear, you must delete it with the **no banner incoming** command.

To customize the banner, use tokens in the form $(*token*) in the message text. Tokens will display current Cisco IOS configuration variables, such as the router's host name and IP address. The tokens are described in Table 8.

Table 8 banner incoming Tokens

Token	Information Displayed in the Banner
$(hostname)	Displays the host name for the router.
$(domain)	Displays the domain name for the router.
$(line)	Displays the vty or tty (asynchronous) line number.
$(line-desc)	Displays the description attached to the line.

Examples

The following example sets an incoming connection banner. The pound sign (#) is used as a delimiting character.

```
Router(config)# banner incoming #
This is the Reuses router.
#
```

The following example sets an incoming connection banner that uses several tokens. The percent sign (%) is used as a delimiting character.

```
darkstar(config)# banner incoming %
Enter TEXT message.  End with the character '%'.
You have entered $(hostname).$(domain) on line $(line) ($(line-desc)) %
```

When the incoming connection banner is executed, the user will see the following banner. Notice that the $(*token*) syntax is replaced by the corresponding configuration variable.

```
You have entered darkstar.ourdomain.com on line 5 (Dialin Modem)
```

Related Commands

Command	Description
banner exec	Defines a customized banner to be displayed whenever the EXEC process is initiated.
banner login	Defines a customized banner to be displayed before the username and password login prompts.
banner motd	Defines a customized message-of-the-day banner.
banner slip-ppp	Defines a customized banner to be displayed when a serial-line IP or point-to-point connection is made.

banner login

To define and enable a customized banner to be displayed before the username and password login prompts, use the **banner login** command in global configuration mode. To disable the login banner, use **no** form of this command.

banner login *d message d*

no banner login

Syntax Description

d	Delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the banner message.
message	Message text. You can include tokens in the form *$(token)* in the message text. Tokens will be replaced with the corresponding configuration variable. Tokens are described in Table 9.

Defaults

Disabled (no login banner is displayed).

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.3(7.5)AA	Token functionality was introduced.
12.0(3)T	Token functionality was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

Follow the **banner login** command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

When a user connects to the router, the message-of-the-day (MOTD) banner (if configured) appears first, followed by the login banner and prompts. After the user successfully logs in to the router, the EXEC banner or incoming banner will be displayed, depending on the type of connection. For a reverse Telnet login, the incoming banner will be displayed. For all other connections, the router will display the EXEC banner.

To customize the banner, use tokens in the form $(*token*) in the message text. Tokens will display current Cisco IOS configuration variables, such as the router's host name and IP address. The tokens are described in Table 9.

Table 9 banner login Tokens

Token	Information Displayed in the Banner
$(hostname)	Displays the host name for the router.
$(domain)	Displays the domain name for the router.

Table 9 banner login Tokens (continued)

Token	Information Displayed in the Banner
$(line)	Displays the vty or tty (asynchronous) line number.
$(line-desc)	Displays the description attached to the line.

Examples

The following example sets a login banner. Double quotes (") are used as the delimiting character.

```
Router# banner login " Access for authorized users only. Please enter your username and
password. "
```

The following example sets a login banner that uses several tokens. The percent sign (%) is used as the delimiting character.

```
darkstar(config)# banner login %
Enter TEXT message. End with the character '%'.
You have entered $(hostname).$(domain) on line $(line) ($(line-desc)) %
```

When the login banner is executed, the user will see the following banner. Notice that the $(token) syntax is replaced by the corresponding configuration variable.

```
You have entered darkstar.ourdomain.com on line 5 (Dialin Modem)
```

Related Commands

Command	Description
banner exec	Defines a customized banner to be displayed whenever the EXEC process is initiated.
banner incoming	Defines a customized message to be displayed when there is an incoming connection to a terminal line from a host on the network.
banner motd	Defines a customized message-of-the-day banner.
banner slip-ppp	Defines a customized banner to be displayed when a serial-line IP or point-to-point connection is made.

banner motd

To define and enable a message-of-the-day (MOTD) banner, use the **banner motd** command in global configuration mode. To delete the MOTD banner, use the **no** form of this command.

banner motd *d message d*

no banner motd

Syntax Description

d	Delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the banner message.
message	Message text. You can include tokens in the form $(*token*) in the message text. Tokens will be replaced with the corresponding configuration variable.

Defaults

Disabled (no MOTD banner is displayed).

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.3(7.5)AA	Token functionality was introduced.
12.0(3)T	Token functionality was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

This MOTD banner is displayed to all terminals connected and is useful for sending messages that affect all users (such as impending system shutdowns). Use the **no exec-banner** or **no motd-banner** command to disable the MOTD banner on a line. The **no exec-banner** command also disables the EXEC banner on the line.

When a user connects to the router, the MOTD banner appears before the login prompt. After the user logs in to the router, the EXEC banner or incoming banner will be displayed, depending on the type of connection. For a reverse Telnet login, the incoming banner will be displayed. For all other connections, the router will display the EXEC banner.

To customize the banner, use tokens in the form $(*token*) in the message text. Tokens will display current Cisco IOS configuration variables, such as the router's host name and IP address. The tokens are described in Table 10.

Table 10 banner motd Tokens

Token	Information Displayed in the Banner
$(hostname)	Displays the host name for the router.
$(domain)	Displays the domain name for the router.
$(line)	Displays the vty or tty (asynchronous) line number.
$(line-desc)	Displays the description attached to the line.

Examples

The following example configures an MOTD banner. The pound sign (#) is used as a delimiting character.

```
Router# banner motd # Building power will be off from 7:00 AM until 9:00 AM this coming
Tuesday. #
```

The following example configures an MOTD banner with a token. The percent sign (%) is used as a delimiting character.

```
darkstar(config)# banner motd %
Enter TEXT message.  End with the character '%'.
Notice: all routers in $(domain) will be upgraded beginning April 20
%
```

When the MOTD banner is executed, the user will see the following. Notice that the $(*token*) syntax is replaced by the corresponding configuration variable.

```
Notice: all routers in ourdomain.com will be upgraded beginning April 20
```

Related Commands

Command	Description
banner exec	Defines and enables a customized banner to be displayed whenever the EXEC process is initiated.
banner incoming	Defines and enables a customized message to be displayed when there is an incoming connection to a terminal line from a host on the network.
banner login	Defines and enables a customized banner to be displayed before the username and password login prompts.
banner slip-ppp	Defines and enables a customized banner to be displayed when a serial-line IP or point-to-point connection is made.
exec-banner	Controls (enables or disables) the display of EXEC banners and message-of-the-day banners on a specified line or lines.
motd-banner	Controls (enables or disables) the display of message-of-the-day banners on a specified line or lines.

banner slip-ppp

To customize the banner that is displayed when a Serial Line Internet Protocol (SLIP) or PPP connection is made, use the **banner slip-ppp** command in global configuration mode. To restore the default SLIP or PPP banner, use the **no** form of this command.

banner slip-ppp *d message d*

no banner slip-ppp

Syntax Description

d	Delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the banner message.
message	Message text. You can include tokens in the form $(*token*) in the message text. Tokens will be replaced with the corresponding configuration variable.

Defaults

The default SLIP or PPP banner message is:

```
Entering encapsulation mode.
Async interface address is unnumbered (Ethernet0)
Your IP address is 10.000.0.0 MTU is 1500 bytes
```

The banner message when using the **service old-slip-prompt** command is:

```
Entering encapsulation mode.
Your IP address is 10.100.0.0 MTU is 1500 bytes
```

where *encapsulation* is SLIP or PPP.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

Use this command to define a custom SLIP or PPP connection message. This is useful when legacy client applications require a specialized connection string. To customize the banner, use tokens in the form $(*token*) in the message text. Tokens will display current Cisco IOS configuration variables, such as the routers host name, IP address, encapsulation type, and Maximum Transfer Unit (MTU) size. The banner tokens are described in Table 11.

Table 11 banner slip-ppp Tokens

Token	Information Displayed in the Banner
$(hostname)	Displays the host name of the router.
$(domain)	Displays the domain name of the router.
$(peer-ip)	Displays the IP address of the peer machine.
$(gate-ip)	Displays the IP address of the gateway machine.
$(encap)	Displays the encapsulation type (SLIP, PPP, and so on).
$(encap-alt)	Displays the encapsulation type as SL/IP instead of SLIP.
$(mtu)	Displays the MTU size.

Examples

The following example sets the SLIP/PPP banner using several tokens and the percent sign (%) as the delimiting character:

```
Router(config)# banner slip-ppp %
Enter TEXT message.  End with the character '%'.
Starting $(encap) connection from $(gate-ip) to $(peer-ip) using a maximum packet size of
$(mtu) bytes... %
```

The new SLIP/PPP banner will now be displayed when the **slip** EXEC command is used. Notice that the $(*token*) syntax is replaced by the corresponding configuration variable.

```
Router# slip
Starting SLIP connection from 172.16.69.96 to 192.168.1.200 using a maximum packet size of
1500 bytes...
```

Related Commands

Command	Description
banner exec	Defines and enables a customized banner to be displayed whenever the EXEC process is initiated.
banner incoming	Defines and enables a customized message to be displayed when there is an incoming connection to a terminal line from a host on the network.
banner motd	Defines and enables a customized message-of-the-day banner.
ppp	Initiates a connection to a remote host using PPP.
slip	Initiates a connection to a remote host using SLIP.

boot

To boot the router manually, use the **boot** command in ROM monitor mode. The syntax of this command varies according to the platform and ROM monitor version.

boot

boot *file-url*

boot *filename* [*tftp-ip-address*]

boot flash [*flash-fs***:**][*partition-number***:**][*filename*]

Cisco 7000 Series, 7200 Series, 7500 Series Routers

boot *flash-fs***:**[*filename*]

Cisco 1600 and Cisco 3600 Series Routers

boot [*flash-fs***:**][*partition-number***:**][*filename*]

Syntax Description

file-url	URL of the image to boot (for example, `boot tftp://172.16.15.112/routertest`).
filename	When used in conjunction with the *ip-address* argument, the *filename* argument is the name of the system image file to boot from a network server. The filename is case sensitive. When used in conjunction with the **flash** keyword, the *filename* argument is the name of the system image file to boot from Flash memory. On all platforms except the Cisco 1600 series, Cisco 3600 series, and Cisco 7000 family routers, the system obtains the image file from internal Flash memory. On the Cisco 1600 series, Cisco 3600 series and Cisco 7000 family routers, the *flash-fs***:** argument specifies the Flash memory device from which to obtain the system image. (See the *flash-fs***:** argument later in this table for valid device values.) The filename is case sensitive. Without the *filename* argument, the first valid file in Flash memory is loaded.
tftp-ip-address	(optional) IP address of the TFTP server on which the system image resides. If omitted, this value defaults to the IP broadcast address of 255.255.255.255.
flash	Boots the router from Flash memory. Note that this keyword is required in some boot images.

flash-fs:	(Optional) Specifying the Flash file system is optional for all platforms except the Cisco 7500 series routers. Possible file systems are: • **flash:**—Internal Flash memory. • **bootflash:**—Internal Flash memory on the Cisco 7000 family. • **slot0:**—Flash memory card in the first PCMCIA slot on the Cisco 7000 family and Cisco 3600 series routers. • **slot1:**—Flash memory card in the second PCMCIA slot on the Cisco 7000 family and Cisco 3600 series routers.
partition-number:	(Optional) Specifies the partition number of the file system the file should be loaded from. This argument is not available on all platforms.

Defaults

For most platforms, if you enter the **boot** command and press Enter, the router boots from ROM by default. However, for some platforms, such as the Cisco 3600 series routers, if you enter the **boot** command and press Return, the router boots the first image in Flash memory. Refer to the documentation for your platform for information about the default image.

If the *partition-number* is not specified, the first partition is used.

If the *filename* is not specified, the first file in the partition or file system is used.

For other defaults, see the "Syntax Description" section.

Command Modes

ROM monitor

Command History

Release	Modification
10.3	The command was introduced.

Usage Guidelines

To determine which form of this command to use, refer to the documentation for your platform or use the CLI help (**?**) feature.

Use this command only when your router cannot find the boot configuration information needed in NVRAM. To enter ROM monitor mode, use one of the following methods:

- Enter the **reload** EXEC command, then press the **Break** key during the first 60 seconds of startup.
- Set the configuration register bits 0 to 3 to zero (for example, set the configuration register to 0x0) and enter the **reload** command.

The ROM Monitor prompt is either ">" or, for newer platforms, "rommon *x*>". Enter only lowercase commands.

These commands work only if there is a valid image to boot. Also, from the ROM monitor prompt, issuing a prior reset command is necessary for the boot to be consistently successful.

Refer to your hardware documentation for information on correct jumper settings for your platform.

Note For some platforms the **flash** keyword is now required. If your attempts to use the boot command are failing using the older **boot flash:***x*:[*filename*] syntax, try using the **boot flash flash:***x*:[*filename*] syntax.

Examples

In the following example, a router is manually booted from ROM:

```
> boot
F3:
(ROM Monitor copyrights)
```

In the following example, a router boots the file named routertest from a network server with the IP address 172.16.15.112 using the *file-url* syntax:

```
> boot tftp://172.16.15.112/routertest
F3
(ROM Monitor copyrights)
```

The following example shows the **boot flash** command without the *filename* argument. The first valid file in Flash memory is loaded.

```
> boot flash
F3: 1858656+45204+166896 at 0x1000
Booting gs7-k from flash memory RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR [OK - 1903912/13765276 bytes]
F3: 1858676+45204+166896 at 0x1000
(ROM Monitor copyrights)
```

The following example boots from Flash memory using the file named gs7-k:

```
> boot flash gs7-k
F3: 1858656+45204+166896 at 0x1000

Booting gs7-k from flash memory RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRR [OK - 1903912/13765276 bytes]
F3: 1858676+45204+166896 at 0x1000

(ROM Monitor copyrights)
```

In the following example, the **boot flash flash:** command boots the relocatable image file named igs-bpx-l from partition 2 in Flash memory:

```
> boot flash flash:2:igs-bpx-l
F3: 3562264+98228+303632 at 0x30000B4

(ROM Monitor copyrights)
```

In the following command, the Cisco 7000 family router accepts the **flash** keyword for compatibility but ignores it, and boots from slot 0:

```
> boot flash slot0:gs7-k-mz.103-9
F3: 8468+3980384+165008 at 0x1000
```

In the following example, the command did not function because it must be entered in lowercase:

```
rommon 10 > BOOT
command "BOOT" not found
```

The following example boots the first file in the first partition of internal Flash memory of a Cisco 3600 series router:

```
> boot flash:
```

The following example boots the first image file in the first partition of the Flash memory card in slot 0 of a Cisco 3600 series router:

```
> boot slot0:
```

The following example shows the ROM monitor booting the first file in the first Flash memory partition on a Cisco 1600 series router:

```
> boot flash:
```

Related Commands

Command	Description
continue	Returns to EXEC mode from ROM monitor mode by completing the boot process.

boot bootldr

To specify the location of the boot image that ROM uses for booting, use the **boot bootldr** command in global configuration mode. To remove this boot image specification, use the **no** form of this command.

boot bootldr *file-url*

no boot bootldr

Syntax Description

file-url	URL of the boot image on a Flash file system.

Defaults

Refer to your platform documentation for the location of the default boot image.

Command Modes

Global configuration

Command History

Release	Modification
11.0	The command was introduced.

Usage Guidelines

The **boot bootldr** command sets the BOOTLDR variable in the current running configuration. You must specify both the Flash file system and the filename.

Note When you use this global configuration command, you affect only the running configuration. You must save the variable setting to your startup configuration to place the information under ROM monitor control and to have the variable function as expected. Use the **copy system:running-config nvram:startup-config** command to save the variable from your running configuration to your startup configuration.

The **no** form of the command sets the BOOTLDR variable to a null string. On the Cisco 7000 family routers, a null string causes the first image file in boot Flash memory to be used as the boot image that ROM uses for booting.

Use the **show boot** command to display the current value for the BOOTLDR variable.

Examples

In the following example, the internal Flash memory contains the boot image:

```
boot bootldr bootflash:boot-image
```

The following example specifies that the Flash memory card inserted in slot 0 contains the boot image:

```
boot bootldr slot0:boot-image
```

Related Commands

Command	Description
copy system:running-config nvram:startup-config	Copies any file from a source to a destination.
show (flash file system)	Displays the layout and contents of a Flash memory file system.
show bootvar	Displays the contents of the BOOT variable, the name of the configuration file pointed to by the CONFIG_FILE variable, the contents of the BOOTLDR variable, and the configuration register setting.

boot bootstrap

To configure the filename that is used to boot a secondary bootstrap image, use the **boot bootstrap** command in global configuration mode. To disable booting from a secondary bootstrap image, use the **no** form of this command.

boot bootstrap *file-url*

no boot bootstrap *file-url*

boot bootstrap flash [*filename*]

no boot bootstrap flash [*filename*]

boot bootstrap [**tftp**] *filename* [*ip-address*]

no boot bootstrap [**tftp**] *filename* [*ip-address*]

Syntax Description

file-url	URL of the bootstrap image.
flash	Boots the router from Flash memory.
filename	(Optional with **flash**) Name of the system image to boot from a network server or from Flash memory. If you omit the filename when booting from Flash memory, the router uses the first system image stored in Flash memory.
tftp	(Optional) Boots the router from a system image stored on a TFTP server.
ip-address	(Optional) IP address of the TFTP server on which the system image resides. If omitted, this value defaults to the IP broadcast address of 255.255.255.255.

Defaults

No secondary bootstrap

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **boot bootstrap** command causes the router to load a secondary bootstrap image from the specied URL, such as from a remote server. After the bootstrap image is loaded, the bootstrap image loads the specified system image file. See the appropriate hardware installation guide for details on the setting the configuration register and secondary bootstrap filename.

Use this command when you have attempted to load a system image but have run out of memory even after compressing the system image. Secondary bootstrap images allows you to load a larger system image through a smaller secondary image.

Examples

In the following example, the system image file named sysimage-2 will be loaded by using a secondary bootstrap image:

```
Router(config)# boot bootstrap bootflash:sysimage-2
```

boot buffersize

The **boot buffersize** global configuration command no longer functions.

Executing this command has no effect on the system. Using this command will not generate CLI errors; the **boot buffersize** command syntax is still allowed to be entered at the CLI and in configuration files in order to accommodate existing configuration scripts used by customers.

Command History

Release	Modification
10.0	This command was introduced.
12.1	Command functionality was removed.

boot config

To specify the device and filename of the configuration file from which the router configures itself during initialization (startup), use the **boot config** command in global configuration mode. This command is only available on Class A file system platforms. To remove the specification, use the **no** form of this command.

boot config *file-system-prefix***:**[*directory*/]*filename*

no boot config

Syntax Description

*file-system-prefix***:**	File system, followed by a colon (for example, **nvram:**, **flash:**, or **slot0:**).
directory/	(Optional) File system directory the configuration file is located in, followed by a forward slash (/).
filename	Name of the configuration file.

Defaults

NVRAM (**nvram:**)

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

This command is only available on Class A file system platforms.

You set the CONFIG_FILE environment variable in the current running memory when you use the **boot config** command. This variable specifies the configuration file used for initialization (startup). The configuration file must be an ASCII file located in either NVRAM or Flash memory.

Note When you use this global configuration command, you affect only the running configuration. You must save the environment variable setting to your startup configuration to place the information under ROM monitor control and to have the environment variable function as expected. Use the **copy system:running-config nvram:startup-config** command to save the environment variable from your running configuration to your startup configuration.

The software displays an error message and does not update the CONFIG_FILE environment variable in the following situations:

- You specify **nvram:** as the file system, and it contains only a distilled version of the configuration. (A distilled configuration is one that does not contain access lists.)
- You specify a configuration file in the *filename* argument that does not exist or is not valid.

The router uses the NVRAM configuration during initialization when the CONFIG_FILE environment variable does not exist or when it is null (such as at first-time startup). If the software detects a problem with NVRAM or the configuration it contains, the device enters setup mode. See the "Setup Command" chapter in this publication for more information on the **setup** command facility.

When you use the **no** form of this command, the router returns to using the default NVRAM configuration file as the startup configuration.

Examples

In the following example, the first line specifies that the router should use the configuration file named *router-config* located in internal Flash memory to configure itself during initialization. The third line copies the specification to the startup configuration, ensuring that this specification will take effect upon the next reload.

```
Router(config)# boot config flash:router-config
Router(config)# end
Router# copy system:running-config nvram:startup-config
```

The following example instructs a Cisco 7500 series router to use the configuration file named *router-config* located on the Flash memory card inserted in the second PCMCIA slot of the RSP card during initialization. The third line copies the specification to the startup configuration, ensuring that this specification will take effect upon the next reload.

```
Router (config)# boot config slot1:router-config
Router (config)# end
Router# copy system:running-config nvram:startup-config
```

Related Commands

Command	Description
show bootvar	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.

boot host

To specify the host-specific configuration file to be used at the next system startup, use the **boot host** command in global configuration mode. To restore the host configuration filename to the default, use the **no** form of this command.

boot host *remote-url*

no boot host *remote-url*

Syntax Description

remote-url	Location of the configuration file. Use the following syntax: • **ftp:**[[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*] • **rcp:**[[[//[*username***@**]*location*]/*directory*]/*filename*] • **tftp:**[[[//*location*]/*directory*]/*filename*]

Defaults

If you do not specify a *filename* using this command, the router uses its configured host name to request a configuration file from a remote server. To form the configuration filename, the router converts its name to all lowercase letters, removes all domain information, and appends *-confg* or *-config*.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command instructs the system to "Boot using host-specific configuration file *x*," where *x* is the filename specified in the *remote-url* argument. In other words, this command specifies the remote location and filename of the host-specific configuration file to be used at the next system startup, as well as the protocol to be used to obtain the file.

Before using the **boot host** command, use the **service config** global configuration command to enable the loading of the specified configuration file at reboot time. Without this command, the router ignores the **boot host** command and uses the configuration information in NVRAM. If the configuration information in NVRAM is invalid or missing, the **service config** command is enabled automatically.

The network server will attempt to load two configuration files from remote hosts. The first is the network configuration file containing commands that apply to all network servers on a network. Use the **boot network** command to identify the network configuration file. The second is the host configuration file containing commands that apply to one network server in particular. Use the **boot host** command to identify the host configuration file.

Loading a Configuration File Using rcp

The rcp software requires that a client send the remote username on each rcp request to the network server. If the server has a directory structure (such as UNIX systems), the rcp implementation searches for the configuration files starting in the directory associated with the remote username.

When you load a configuration file from a server using rcp, the Cisco IOS software sends the first valid username in the following list:

1. The username specified in the file-URL, if a username is specified.
2. The username set by the **ip rcmd remote-username** command, if the command is configured.
3. The router host name.

Note An account for the username must be defined on the destination server. If the network administrator of the destination server did not establish an account for the username, this command will not execute successfully.

Loading a Configuration File Using FTP

The FTP protocol requires a client to send a remote username and password on each FTP request to a server. The username and password must be associated with an account on the FTP server. If the server has a directory structure, the configuration file or image copied from the directory is associated with the username on the server. Refer to the documentation for your FTP server for more details.

When you load a configuration file from a server using FTP, the Cisco IOS software sends the first valid username in the following list:

1. The username specified in the **boot host** command, if a username is specified.
2. The username set by the **ip ftp username** command, if the command is configured.
3. Anonymous.

The router sends the first valid password in the following list:

1. The password specified in the **boot host** command, if a password is specified.
2. The password set by the **ip ftp password** command, if the command is configured.
3. The router forms a password *username@routername.domain*. The variable *username* is the username associated with the current session, *routername* is the configured host name, and *domain* is the domain of the router.

Examples

The following example sets the host filename to wilma-confg at address 192.168.7.19:

```
Router(config)# boot host tftp://192.168.7.19/usr/local/tftpdir/wilma-confg
Router(config)# service config
```

Related Commands

Command	Description
boot network	Specifies the remote location and filename of the network configuration file to be used at the next system boot (startup).
service config	Enables autoloading of configuration files from a network server.

boot network

To change the default name of the network configuration file from which to load configuration commands, use the **boot network** command in global configuration mode. To restore the network configuration filename to the default, use the **no** form of this command.

boot network *remote-url*

no boot network *remote-url*

Syntax Description

remote-url	Location of the configuration file. Use the following syntax: • **ftp:**[[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*] • **rcp:**[[[//[*username***@**]*location*]/*directory*]/*filename*] • **tftp:**[[[//*location*]/*directory*]/*filename*]

Defaults

The default *filename* is network-config.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command instructs the system to "Boot using network configuration file *x*," where *x* is the filename specified in the *remote-url* argument. This command specifies the remote location and filename of the network configuration file to be used at the next system startup, as well as the protocol to be used to obtain the file.

When booting from a network server, routers ignore routing information, static IP routes, and bridging information. As a result, intermediate routers are responsible for handling FTP, rcp, or TFTP requests. Before booting from a network server, verify that a server is available by using the **ping** command.

Use the **service config** command to enable the loading of the specified configuration file at reboot time. Without this command, the router ignores the **boot network** command and uses the configuration information in NVRAM. If the configuration information in NVRAM is invalid or missing, the **service config** command is enabled automatically.

The network server will attempt to load two configuration files from remote hosts. The first is the network configuration file containing commands that apply to all network servers on a network. Use the **boot network** command to identify the network configuration file. The second is the host configuration file containing commands that apply to one network server in particular. Use the **boot host** command to identify the host configuration file.

Loading a Configuration File Using rcp

The rcp software requires that a client send the remote username on each rcp request to the network server. If the server has a directory structure (such as UNIX systems), the rcp implementation searches for the configuration files starting in the directory associated with the remote username.

When you load a configuration file from a server using rcp, the Cisco IOS software sends the first valid username in the following list:

1. The username specified in the file-URL, if a username is specified.
2. The username set by the **ip rcmd remote-username** command, if the command is configured.
3. The router host name.

Note An account for the username must be defined on the destination server. If the network administrator of the destination server did not establish an account for the username, this command will not execute successfully.

Loading a Configuration File Using FTP

The FTP protocol requires a client to send a remote username and password on each FTP request to a server. The username and password must be associated with an account on the FTP server. If the server has a directory structure, the configuration file or image copied from the directory associated with the username on the server. Refer to the documentation for your FTP server for more details.

When you load a configuration file from a server using FTP, the Cisco IOS software sends the first valid username in the following list:

1. The username specified in the **boot network** command, if a username is specified.
2. The username set by the **ip ftp username** command, if the command is configured.
3. Anonymous.

The router sends the first valid password in the following list:

1. The password specified in the **boot network** command, if a password is specified.
2. The password set by the **ip ftp password** command, if the command is configured.
3. The router forms a password *username@routername.domain*. The variable *username* is the username associated with the current session, *routername* is the configured host name, and *domain* is the domain of the router.

Examples

The following example changes the network configuration filename to bridge_9.1 and uses the default broadcast address:

```
Router(config)# boot network tftp:bridge_9.1
Router(config)# service config
```

The following example changes the network configuration filename to bridge_9.1, specifies that rcp is to be used as the transport mechanism, and gives 172.16.1.111 as the IP address of the server on which the network configuration file resides:

```
Router(config)# service config
Router(config)# boot network rcp://172.16.1.111/bridge_9.1
```

Related Commands

Command	Description
boot host	Specifies the remote location and filename of the host-specific configuration file to be used at the next system boot (startup).
service config	Enables autoloading of configuration files from a remote host.

boot system

To specify the system image that the router loads at startup, use one of the following **boot system** commands in global configuration mode. To remove the startup system image specification, use the **no** form of the command.

boot system *file-url*

no boot system *file-url*

boot system flash [*flash-fs***:**][*partition-number***:**][*filename*]

no boot system flash [*flash-fs***:**][*partition-number***:**][*filename*]

boot system mop *filename* [*mac-address*] [*interface*]

no boot system mop *filename* [*mac-address*] [*interface*]

boot system rom

no boot system rom

boot system {**rcp** | **tftp** | **ftp**} *filename* [*ip-address*]

no boot system {**rcp** | **tftp** | **ftp**} *filename* [*ip-address*]

no boot system

Syntax Descriptionn

file-url	URL of the system image to load at system startup.
flash	On all platforms except the Cisco 1600 series, Cisco 3600 series, and Cisco 7000 family routers, this keyword boots the router from internal Flash memory. If you omit all arguments that follow this keyword, the system searches internal Flash for the first bootable image. On the Cisco 1600 series, Cisco 3600 series, and Cisco 7000 family routers, this keyword boots the router from a Flash device, as specified by the *device*: argument. On the Cisco 1600 series and Cisco 3600 series routers, if you omit all optional arguments, the router searches internal Flash memory for the first bootable image. On the Cisco 7000 family routers, when you omit all arguments that follow this keyword, the system searches the PCMCIA slot 0 for the first bootable image.

*flash-fs***:**	(Optional) Flash file system containing the system image to load at startup. The colon is required. Valid file systems are as follows: • **flash:**—Internal Flash memory on the Cisco 1600 series and Cisco 3600 series routers. For the Cisco 1600 series and Cisco 3600 series routers, this file system is the default if you do not specify a file system. This is the only valid file system for the Cisco 1600 series. • **bootflash:**—Internal Flash memory in the Cisco 7000 family. • **slot0:**—First PCMCIA slot on the Cisco 3600 series and Cisco 7000 family routers. For the Cisco 7000 family routers, this file system is the default if you do not specify a file system. • **slot1:**—Flash memory card in the second PCMCIA slot on the Cisco 3600 series and Cisco 7000 family routers.
*partition-number***:**	(Optional) Number of the Flash memory partition that contains the system image to boot, specified by the optional *filename* argument. If you do not specify a filename, the router loads the first valid file in the specified partition of Flash memory. This argument is only valid on routers that can be partitioned.
filename	(Optional when used with the **boot system flash** command) Name of the system image to load at startup. It is case sensitive. If you do not specify a filename, the router loads the first valid file in the specified Flash file system, the specified partition of Flash memory, or the default Flash file system if you also omit the *flash-fs***:** argument.
mop	Boots the router from a system image stored on a DECNET Maintenance Operations Protocol (MOP) server. Do not use this keyword with the Cisco 3600 series or Cisco 7000 family routers.
mac-address	(Optional) MAC address of the MOP server containing the specified system image file. If you do not include the MAC address argument, the router sends a broadcast message to all MOP boot servers. The first MOP server to indicate that it has the specified file is the server from which the router gets the boot image.
interface	(Optional) Interface the router uses to send out MOP requests to the MOP server. The interface options are **async**, **dialer**, **ethernet**, **serial**, and **tunnel**. If you do not specify the *interface* argument, the router sends a request out on all interfaces that have MOP enabled. The interface that receives the first response is the interface the router uses to load the software.
rom	Boots the router from ROM. Do not use this keyword with the Cisco 3600 series or the Cisco 7000 family routers.
rcp	Boots the router from a system image stored on a network server using rcp.
tftp	Boots the router from a system image stored on a TFTP server.
ftp	Boots the router from a system image stored on an FTP server.
ip-address	(Optional) IP address of the server containing the system image file. If omitted, this value defaults to the IP broadcast address of 255.255.255.255.

Defaults

If you configure the router to boot from a network server but do not specify a system image file with the **boot system** command, the router uses the configuration register settings to determine the default system image filename. The router forms the default boot filename by starting with the word *cisco* and then appending the octal equivalent of the boot field number in the configuration register, followed by a hyphen (-) and the processor type name (cisco*nn-cpu*). Refer to the appropriate hardware installation guide for details on the configuration register and default filename. See also the **config-register** or **confreg** command. For additional information about defaults, see the preceding "Syntax Description" section.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

For this command to work, the **config-register** command must be set properly.

Enter several **boot system** commands to provide a fail-safe method for booting your router. The router stores and executes the **boot system** commands in the order in which you enter them in the configuration file. If you enter multiple boot commands of the same type—for example, if you enter two commands that instruct the router to boot from different network servers—then the router tries them in the order in which they appear in the configuration file. If a **boot system** command entry in the list specifies an invalid device, the router omits that entry. Use the **boot system rom** command to specify use of the ROM system image as a backup to other **boot** commands in the configuration.

For some platforms, the boot image must be loaded before the system image is loaded. However, on many platforms, the boot image is loaded only if the router is booting from a network server or if the Flash file system is not specified. If the file system is specified, the router will boot faster because it need not load the boot image first.

This section contains the following usage guideline sections:

- Changing the List of Boot System Commands
- Booting Compressed Images
- Understanding rcp
- Stopping Booting and Enter ROM Monitor Mode
- Cisco 1600 Series, Cisco 3600 Series, and Cisco 7000 Family Router Notes

Changing the List of Boot System Commands

To remove a single entry from the bootable image list, use the **no** form of the command with an argument. For example, to remove the entry that specifies a bootable image on a Flash memory card inserted in the second slot, use the **no boot system flash slot1:**[*filename*] command. All other entries in the list remain.

To eliminate all entries in the bootable image list, use the **no boot system** command. At this point, you can redefine the list of bootable images using the previous **boot system** commands. Remember to save your changes to your startup configuration by issuing the **copy system:running-config nvram:startup-config** command.

Each time you write a new software image to Flash memory, you must delete the existing file name in the configuration file with the **no boot system flash** *filename* command. Then add a new line in the configuration file with the **boot system flash** *filename* command.

Note If you want to rearrange the order of the entries in the configuration file, you must first issue the **no boot system** command and then redefine the list.

Booting Compressed Images

You can boot the router from a compressed image on a network server. When a network server boots software, both the image being booted and the running image must fit into memory. Use compressed images to ensure that enough memory is available to boot the router. You can compress a software image on any UNIX platform using the **compress** command. Refer to your UNIX platform's documentation for the exact usage of the **compress** command. (You can also uncompress data with the UNIX **uncompress** command.)

Understanding rcp

The rcp requires that a client send the remote username in an rcp request to a server. When the router executes the **boot system rcp** command, the Cisco IOS software sends the host name as both the remote and local usernames by default. For the rcp to execute properly, an account must be defined on the network server for the remote username configured on the router.

If the server has a directory structure, the rcp software searches for the system image to boot from the remote server relative to the directory of the remote username.

By default, the router software sends host name as the remote username. You can override the default remote username by using the **ip rcmd remote-username** command. For example, if the system image resides in the home directory of a user on the server, you can specify that user's name as the remote username.

Understanding TFTP

You need a TFTP server running in order to retrieve the router image from the host.

Understanding FTP

You need to an FTP server running in order to fetch the router image from the host. You also need an account on the server or anonymous file access to the server.

Stoping Booting and Entering ROM Monitor Mode

During the first 60 seconds of startup, you can force the router to stop booting by pressing the Break key. The router will enter ROM Monitor mode, where you can change the configuration register value or boot the router manually.

Cisco 1600 Series, Cisco 3600 Series, and Cisco 7000 Family Router Notes

For the Cisco 3600 series and Cisco 7000 family, the **boot system** command modifies the BOOT variable in the running configuration. The BOOT variable specifies a list of bootable images on various devices.

Note When you use the **boot system** global configuration command on the Cisco 1600 series, Cisco 3600 series, and Cisco 7000 family, you affect only the running configuration. You must save the BOOT variable settings to your startup configuration to place the information under ROM monitor control and to have the variable function as expected. Use the **copy system:running-config nvram:startup-config** EXEC command to save the variable from your running configuration to your startup configuration.

To view the contents of the BOOT variable, use the **show bootenv** EXEC command.

Examples

The following example illustrates a configuration that specifies two possible internetwork locations for a system image, with the ROM software being used as a backup:

```
Router(config)# boot system tftp://192.168.7.24/cs3-rx.90-1
Router(config)# boot system tftp://192.168.7.19/cs3-rx.83-2
Router(config)# boot system rom
```

The following example boots the system boot relocatable image file named igs-bpx-l from partition 2 of the Flash device:

```
Router(config)# boot system flash:2:igs-bpx-l
```

The following example instructs the router to boot from an image located on the Flash memory card inserted in slot 0:

```
Router(config)# boot system slot0:new-config
```

The following example specifies the file named new-ios-image as the system image for a Cisco 3600 series router to load at startup. This file is located in the fourth partition of the Flash memory card in slot 0.

```
Router(config)# boot system slot0:4:dirt/images/new-ios-image
```

This example boots from the image file named c1600-y-l in partition 2 of Flash memory of a Cisco 1600 series router:

```
Router(config)# boot system flash:2:c1600-y-l
```

Related Commands

Command	Description
config-register	Changes the configuration register settings.
copy	Copies any file from a source to a destination.
ip rcmd remote username	Configures the remote username to be used when requesting a remote copy using rcp.
show bootvar	Displays the contents of the BOOT variable, the name of the configuration file pointed to by the CONFIG_FILE variable, the contents of the BOOTLDR variable, and the configuration register setting

boot-end-marker

The **boot-start-marker** and **boot-end-marker** flags, which can be seen in Cisco IOS software configuration files, are not CLI commands. These markers are written to configuration files automatically to flag the beginning and end of the boot commands (boot statements). By flagging boot statements, these markers allow the router to more reliably load Cisco IOS images during bootup.

A boot statement is one or more lines in a configuration file that tells the router which software image to load after a powercycling (reboot). The boot-start-marker and boot-end-marker flags will appear around any boot commands, including:

- **boot bootstrap**
- **boot config**
- **boot host**
- **boot network**
- **boot system**

Note, however, that these markers will always appear in the output of the **show running-config** or **more system:running-config** commands, regardless of whether any actual boot commands have been entered. This means that no boot commands will appear between the markers if no boot commands have been entered, or if all boot commands have been removed from the configuration, as shown in the "Examples" section.

The **boot-start-marker** and **boot-end-marker** flags cannot be removed or modified using the CLI. These markers are written to the startup configuration file whenever a **copy running-config startup-config** command is issued.

These flags were also introduced to circumvent errors in the configuration file, such as a leading space before a boot command (such as those sometimes introduced by manually edited configuration files), or the use of text strings that include the word "boot" in banners or other user-specified text.

If the "boot start-marker" flag is not found in the configuration file, the system will use the traditional method to identify the boot commands. However, if you are manually creating configuration files, or copying from older Cisco IOS software releases, the addition of these markers is recommended.

Command History

Release	Modification
12.3(3), 12.3(4)T, 12.0(26)S, 12.0(27)SV, 12.3(3)B,	The **boot-start-marker** and **boot-end-marker** flags were introduced.

Examples

In the following example, a **boot** command is entered, and the boot-start-marker and boot-end-marker flags are shown in the context of the startup configuration file:

```
Router# configure terminal
Enter configuration commands, one per line.  End with the end command.

Router(config)# boot system slot0:
Router(config)# end
Router# copy running-config startup-config
Router# show startup-config

Using 1398 out of 129016 bytes
```

```
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname C3660-2
!
boot-start-marker
boot system slot0:
boot-end-marker
!
logging count
 .
 .
 .
```

In the following example, the boot-start-marker and boot-end-marker flags appear in the configuration file even though no **boot** commands have been entered:

```
Router# show running-configuration

Current configuration :3055 bytes
!
! No configuration change since last restart
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
 .
 .
 .
```

Related Commands

Command	Description
boot bootstrap	Specifies the filename and location of a secondary bootstrap image (to be used if a valid software image cannot be loaded).
boot config	Specifies the device and filename of the configuration file from which the router boots during startup (for Class A filesytems).
boot host	Specifies a remote host location for the host-specific (router-specific) configuration file to be used at the next system startup.
boot network	Specifies a remote location for the network (network-wide) configuration file to be used at the next system startup.
boot system	Specifies the system software image that the router loads at startup.

boot-start-marker

The **boot-start-marker** and **boot-end-marker** flags, which can be seen in Cisco IOS software configuration files, are not CLI commands. These markers are written to configuration files automatically to flag the beginning and end of the boot commands (boot statements). By flagging boot statements, these markers allow the router to more reliably load Cisco IOS images during bootup.

A boot statement is one or more lines in a configuration file that tells the router which software image to load after a powercycling (reboot). The boot-start-marker and boot-end-marker flags will appear around any boot commands, including:

- **boot bootstrap**
- **boot config**
- **boot host**
- **boot network**
- **boot system**

Note, however, that these markers will always appear in the output of the **show running-config** or **more system:running-config** commands, regardless of whether any actual boot commands have been entered. This means that no boot commands will appear between the markers if no boot commands have been entered, or if all boot commands have been removed from the configuration, as shown in the "Examples" section.

The **boot-start-marker** and **boot-end-marker** flags cannot be removed or modified using the CLI. These markers are written to the startup configuration file whenever a **copy running-config startup-config** command is issued.

These flags were also introduced to circumvent errors in the configuration file, such as a leading space before a boot command (such as those sometimes introduced by manually edited configuration files), or the use of text strings that include the word "boot" in banners or other user-specified text.

If the "boot start-marker" flag is not found in the configuration file, the system will use the traditional method to identify the boot commands. However, if you are manually creating configuration files, or copying from older Cisco IOS software releases, the addition of these markers is recommended.

Command History

Release	Modification
12.3(3), 12.3(4)T, 12.0(26)S, 12.0(27)SV, 12.3(3)B	The **boot-start-marker** and **boot-end-marker** flags were introduced.

Examples

In the following example, a **boot** command is entered, and the boot-start-marker and boot-end-marker flags are shown in the context of the startup configuration file:

```
Router# configure terminal
Enter configuration commands, one per line.  End with the end command.

Router(config)# boot system slot0:
Router(config)# end
Router# copy running-config startup-config
Router# show startup-config

Using 1398 out of 129016 bytes
```

```
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname C3660-2
!
boot-start-marker
boot system slot0:
boot-end-marker
!
logging count
 .
 .
 .
```

In the following example, the boot-start-marker and boot-end-marker flags appear in the configuration file even though no **boot** commands have been entered:

```
Router# show running-configuration

Current configuration :3055 bytes
!
! No configuration change since last restart
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
 .
 .
 .
```

Related Commands

Command	Description
boot bootstrap	Specifies the filename and location of a secondary bootstrap image (to be used if a valid software image cannot be loaded).
boot config	Specifies the device and filename of the configuration file from which the router boots during startup (for Class A filesytems).
boot host	Specifies a remote host location for the host-specific (router-specific) configuration file to be used at the next system startup.
boot network	Specifies a remote location for the network (network-wide) configuration file to be used at the next system startup.
boot system	Specifies the system software image that the router loads at startup.

buckets-of-history-kept

To set the number of history buckets that are kept during a Service Assurance Agent (SAA) operation's lifetime, use the **buckets-of-history-kept** command in SAA RTR configuration mode. To return to the default value, use the **no** form of this command.

buckets-of-history-kept *size*

no buckets-of-history-kept

Syntax Description

size	Number of history buckets kept during the lifetime of the operation. The default is 50 buckets.

Defaults

50 buckets

Command Modes

SAA RTR configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

History collection and statistics capturing is enabled for the following SAA operations: ICMP Echo, SNA Echo, ICMP PathEcho, UDP Echo, TcpConnect, DNS, and DLSW. History collection is not supported for HTTP and Jitter (UDP+) operations.

By default, history is not collected. When a problem arises where history is useful (for example, a large number of timeouts are occurring), you can configure the **lives-of-history-kept** SAA RTR configuration command to collect history. You can optionally adjust the **buckets-of-history-kept**, **filter-for-history**, and **samples-of-history-kept** SAA RTR configuration commands.

When the number of buckets reaches the size specified, no further history for this life is stored.

Note Collecting history increases the RAM usage. Only collect history when you think there is a problem in the network. For general network response time information, use the statistics gathering feature of SAA.

If history is collected, each bucket contains one or more history entries from the operation. When the operation type is pathEcho, an entry is created for each hop along the path that the operation takes to reach its destination. The type of entry stored in the history table is controlled by the **filter-for-history** SAA RTR configuration command. The total number of entries stored in the history table is controlled by the combination of **samples-of-history-kept**, **buckets-of-history-kept**, and **lives-of-history-kept** SAA RTR configuration commands.

Each time the SAA starts an operation, a new bucket is created until the number of history buckets matches the specified size or the operation's lifetime expires. History buckets do not wrap. The operation's lifetime is defined by the **rtr schedule** global configuration command. The operation starts an SAA operation based on the seconds specified by the **frequency** SAA RTR configuration command.

Examples

The following example configures operation 1 to keep 25 history buckets during the operation lifetime:

```
Router(config)# rtr 1
Router(config-rtr)# type echo protocol ipIcmpEcho 172.16.161.21
Router(config-rtr)# buckets-of-history-kept 25
Router(config-rtr)# lives-of-history-kept 1
```

Related Commands

Command	Description
filter-for-history	Defines the type of information kept in the history table for the SA Agent operation.
lives-of-history-kept	Sets the number of lives maintained in the history table for the SA Agent operation.
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.
rtr schedule	Configures the time parameters for an SAA operation.
samples-of-history-kept	Sets the number of entries kept in the history table per bucket for the SA Agent operation.

buffer-length

To specify the maximum length of the data stream to be forwarded, use the **buffer-length** command in line configuration mode. To restore the default setting, use the **no** form of this command.

buffer-length *length*

no buffer-length

Syntax Description

length	Specifies the length of the buffer in bytes. Valid values for the *length* argument range from 16 to 1536. The default buffer length is 1536 bytes.

Defaults

1536 bytes

Command Modes

Line configuration

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

The **buffer-length** command configures the size of the forwarded data stream. The higher the value used for the *length* argument is, the longer the delay between data transmissions will be. Configuring a smaller buffer length can prevent connections from timing out inappropriately.

Examples

The following example configures a buffer length of 500 bytes:

```
Router(config)# line 1
Router(config-line)# buffer-length 500
```

buffers

To make adjustments to initial buffer pool settings and to the limits at which temporary buffers are created and destroyed, use the **buffers** command in global configuration mode. To return the buffers to their default size, use the **no** form of this command.

buffers {**small** | **middle** | **big** | **verybig** | **large** | **huge** | *type number*} {**permanent** | **max-free** | **min-free** | **initial**} *number-of-buffers*

no buffers {**small** | **middle** | **big** | **verybig** | **large** | **huge** | *type number*} {**permanent** | **max-free** | **min-free** | **initial**} *number-of-buffers*

Syntax Description

small	Buffer size of this public buffer pool is 104 bytes.
middle	Buffer size of this public buffer pool is 600 bytes.
big	Buffer size of this public buffer pool is 1524 bytes.
verybig	Buffer size of this public buffer pool is 4520 bytes.
large	Buffer size of this public buffer pool is 5024 bytes.
huge	Default buffer size of this public buffer pool is 18024 bytes. This value can be configured with the **buffers huge size** command.
type number	Interface type and interface number of the interface buffer pool. The *type* value cannot be **fddi**.
permanent	Number of permanent buffers that the system tries to create and keep. Permanent buffers are normally not trimmed by the system.
max-free	Maximum number of free or unallocated buffers in a buffer pool. A maximum of 20,480 small buffers can be constructed in the pool.
min-free	Minimum number of free or unallocated buffers in a buffer pool.
initial	Number of additional temporary buffers that are to be allocated when the system is reloaded. This keyword can be used to ensure that the system has necessary buffers immediately after reloading in a high-traffic environment.
number-of-buffers	Number of buffers to be allocated.

Defaults

The default number of buffers in a pool is determined by the hardware configuration and can be displayed with the **show buffers** EXEC command.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Normally you need not adjust these parameters; do so only after consulting with technical support personnel.

Note Improper buffer settings can adversely impact system performance.

You cannot configure FDDI buffers.

Examples

Examples of Public Buffer Pool Tuning

The following example keeps at least 50 small buffers free in the system:

```
Router(config)# buffers small min-free 50
```

The following example increases the permanent buffer pool allocation for big buffers to 200:

```
Router(config)# buffers big permanent 200
```

Example of Interface Buffer Pool Tuning

A general guideline is to display buffers with the **show buffers** command, observe which buffer pool is depleted, and increase that one.

The following example increases the permanent Ethernet interface 0 buffer pool on a Cisco 4000 router to 96 when the Ethernet 0 buffer pool is depleted:

```
Router(config)# buffers ethernet 0 permanent 96
```

Related Commands

Command	Description
load-interval	Changes the length of time for which data is used to compute load statistics.
show buffers	Displays statistics for the buffer pools on the network server.

buffers huge size

To dynamically resize all huge buffers to the value you specify, use the **buffers huge size** command in global configuration mode. To restore the default buffer values, use the **no** form of this command.

buffers huge size *number-of-bytes*

no buffers huge size *number-of-bytes*

Syntax Description

number-of-bytes	Huge buffer size (in bytes). Valid range is from 18024 to 100000 bytes.

Defaults

18,024 bytes

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command only after consulting with technical support personnel. The buffer size cannot be lowered below the default.

Note Improper buffer settings can adversely impact system performance.

Examples

The following example resizes huge buffers to 20,000 bytes:

```
Router(config)# buffers huge size 20000
```

Related Commands

Command	Description
buffers	Adjusts the initial buffer pool settings and the limits at which temporary buffers are created and destroyed.
show buffers	Displays statistics for the buffer pools on the network server.

calendar set

To manually set the hardware clock (calendar), use one of the formats of the **calendar set** command in EXEC mode.

calendar set *hh:mm:ss day month year*

calendar set *hh:mm:ss month day year*

Syntax Description

hh:mm:ss	Current time in hours (using 24-hour notation), minutes, and seconds.
day	Current day (by date) in the month.
month	Current month (by name).
year	Current year (no abbreviation).

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Some platforms have a hardware clock that is separate from the software clock. In Cisco IOS software syntax, the hardware clock is called the "calendar." The hardware clock is a battery-powered chip that runs continuously, even if the router is powered off or rebooted. After you set the hardware clock, the software clock will be automatically set from the hardware clock when the system is restarted or when the **clock read-calendar** EXEC command is issued. The time specified in this command is relative to the configured time zone.

Examples

The following example manually sets the hardware clock to 1:32 p.m. on May 19, 2003:

```
Router# calendar set 13:32:00 May 19 2003
```

Related Commands

Command	Description
clock read-calendar	Performs a one-time update of the software clock from the hardware clock (calendar).
clock set	Sets the software clock.
clock summer-time	Configures the system time to automatically switch to summer time (daylight saving time).
clock timezone	Sets the time zone for display purposes.
clock update-calendar	Performs a one-time update of the hardware clock from the software clock.

cd

To change the default directory or file system, use the **cd** command in EXEC mode.

cd [*filesystem***:**]

Syntax Description

*filesystem***:**	(Optional) The URL or alias of the directory or file systems followed by a colon.

Defaults

The initial default file system is **flash:**. For platforms that do not have a physical device named **flash:**, the keyword **flash:** is aliased to the default Flash device.

If you do not specify a directory on a file system, the default is the root directory on that file system.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

For all EXEC commands that have an optional *filesystem* argument, the system uses the file system specified by the **cd** command when you omit the optional *filesystem* argument. For example, the **dir** EXEC command, which displays a list of files on a file system, contain an optional *filesystem* argument. When you omit this argument, the system lists the files on the file system specified by the **cd** command.

Examples

In the following example, the **cd** command is used to set the default file system to the Flash memory card inserted in slot 0:

```
Router# pwd
bootflash:/
Router# cd slot0:
Router# pwd
slot0:/
```

Related Commands

Command	Description
copy	Copies any file from a source to a destination.
delete	Deletes a file on a Flash memory device.
dir	Displays a list of files on a file system.
pwd	Displays the current setting of the **cd** command.
show file systems	Lists available file systems and their alias prefix names.
undelete	Recovers a file marked “deleted” on a Class A or Class B Flash file system.

cdp advertise-v2

To enable Cisco Discovery Protocol Version 2 (CDPv2) advertising functionality on a device, use the **cdp advertise-v2** command in global configuration mode. To disable advertising CDPv2 functionality, use the **no** form of the command.

cdp advertise-v2

no cdp advertise-v2

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

CDP Version 2 has three additional type-length values (TLVs): VTP Management Domain Name, Native VLAN, and full/half-Duplex.

Examples

In the following example, CDP Version 2 advertisements are disabled on the router:

```
Router# show cdp
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is  enabled
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# no cdp advertise-v2
Router(config)# end
Router# show cdp
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is not enabled
Router#
```

Related Commands

Command	Description
cdp enable	Enables CDP on a supported interface.
cdp run	Reenables CDP on a Cisco device.

cdp enable

To enable Cisco Discovery Protocol (CDP) on an interface, use the **cdp enable** command in interface configuration mode. To disable CDP on an interface, use the **no** form of this command.

cdp enable

no cdp enable

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled at the global level and on all supported interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

CDP is enabled by default at the global level and on each supported interface in order to send or receive CDP information. However, some interfaces, such as ATM interfaces, do not support CDP.

Note The **cdp enable**, **cdp timer**, and **cdp run** commands affect the operation of the IP on demand routing feature (that is, the **router odr** global configuration command). For more information on the **router odr** command, see the "On-Demand Routing Commands" chapter in the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* document.

Examples

In the following example, CDP is disabled on the Ethernet 0 interface only:

```
Router# show cdp
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is  enabled
Router# config terminal
Router(config)# interface ethernet 0
Router(config-if)# no cdp enable
```

Related Commands

Command	Description
cdp run	Reenables CDP on a Cisco device.
cdp timer	Specifies how often the Cisco IOS software sends CDP updates.
router odr	Enables on-demand routing on a hub router.

cdp holdtime

To specify the amount of time the receiving device should hold a Cisco Discovery Protocol (CDP) packet from the router before discarding it, use the **cdp holdtime** command in global configuration mode. To revert to the default setting, use the **no** form of this command.

cdp holdtime *seconds*

no cdp holdtime

Syntax Description

seconds	Specifies the hold time to be sent in the CDP update packets. The default is 180 seconds.

Defaults

180 seconds

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

CDP packets are sent with a time to live, or hold time, value. The receiving device will discard the CDP information in the CDP packet after the hold time has elapsed.

You can set the hold time lower than the default setting of 180 seconds if you want the receiving devices to update their CDP information more rapidly.

The CDP hold time must be set to a higher number of seconds than the time between CDP transmissions, which is set using the **cdp timer** command.

Examples

In the following example, the CDP packets being sent from the router are configured with a hold time of 60 seconds.

```
Router(config)# cdp holdtime 60
```

Related Commands

Command	Description
cdp timer	Specifies how often the Cisco IOS software sends CDP updates.
show cdp	Displays global CDP information, including timer and hold-time information.

cdp run

To enable Cisco Discovery Protocol (CDP), use the **cdp run** command in global configuration mode. To disable CDP, use the **no** form of this command.

cdp run

no cdp run

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

CDP is enabled by default, which means the Cisco IOS software will receive CDP information. CDP also is enabled on supported interfaces by default. To disable CDP on an interface, use the **no cdp enable** interface configuration command.

Note Because ODR (on demand routing) uses CDP, the **cdp enable**, **cdp timer**, and **cdp run** commands affect the operation of the **router odr** global configuration command. For more information on the **router odr** command, see the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* document.

Examples

In the following example, CDP is disabled globally, then the user attempts to enable CDP on the Ethernet 0 interface:

```
Router(config)# no cdp run
Router(config)# end
Router# show cdp
% CDP is not enabled
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# int eth0
Router(config-if)# cdp enable
% Cannot enable CDP on this interface, since CDP is not running
Router(config-if)#
```

Related Commands

Command	Description
cdp enable	Enables CDP on a supported interface.
cdp timer	Specifies how often the Cisco IOS software sends CDP updates.
router odr	Enables ODR on the hub router.

cdp timer

To specify how often the Cisco IOS software sends Cisco Discovery Protocol (CDP) updates, use the **cdp timer** command in global configuration mode. To revert to the default setting, use the **no** form of this command.

cdp timer *seconds*

no cdp timer

Syntax Description

seconds	Specifies how often the Cisco IOS software sends CDP updates. The default is 60 seconds.

Defaults

60 seconds

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The trade-off with sending more frequent CDP updates to provide up-to-date information, is that bandwidth is used more often.

Note The **cdp enable**, **cdp timer**, and **cdp run** commands affect the operation of the IP on demand routing feature (that is, the **router odr** global configuration command). For more information on the **router odr** command, see the "On-Demand Routing Commands" chapter in the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* document.

Examples

In the following example, CDP updates are sent every 80 seconds, less frequently than the default setting of 60 seconds. You might want to make this change if you are concerned about preserving bandwidth.

```
cdp timer 80
```

Related Commands

Command	Description
cdp enable	Enables CDP on a supported interface.
cdp holdtime	Specifies the amount of time the receiving device should hold a CDP packet from your router before discarding it.
cdp timer	Specifies how often the Cisco IOS software sends CDP updates.

Command	Description
router odr	Enables ODR on the hub router.
show cdp	Displays global CDP information, including timer and hold-time information.

clear cdp counters

To reset Cisco Discovery Protocol (CDP) traffic counters to zero, use the **clear cdp counters** command in privileged EXEC mode.

clear cdp counters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.

Examples

The following example clears the CDP counters. The **show cdp traffic** output shows that all of the traffic counters have been reset to zero.

```
Router# clear cdp counters
Router# show cdp traffic

CDP counters:
        Packets output: 0, Input: 0
        Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
        No memory: 0, Invalid packet: 0, Fragmented: 0
```

Related Commands

Command	Description
clear cdp table	Clears the table that contains CDP information about neighbors.
show cdp traffic	Displays traffic information from the CDP table.

clear cdp table

To clear the table that contains Cisco Discovery Protocol (CDP) information about neighbors, use the **clear cdp table** command in privileged EXEC mode.

clear cdp table

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.

Examples

The following example clears the CDP table. The output of the **show cdp neighbors** command shows that all information has been deleted from the table.

```
Router# clear cdp table

CDP-AD: Deleted table entry for neon.cisco.com, interface Ethernet0
CDP-AD: Deleted table entry for neon.cisco.com, interface Serial0

Router# show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
```

Related Commands

Command	Description
show cdp neighbors	Displays information about neighbors.

clear cns config stats

To clear the statistics about the CNS configuration agent, use the **clear cns config stats** command in privileged EXEC mode.

clear cns config stats

Syntax Description

This command has no arguments or keywords.

Defaults

No statistics are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

The **clear cns config stats** command clears all the statistics displayed by the **show cns config stats** command.

Examples

The following example shows how to clear all of the statistics for the CNS configuration agent:

```
Router# clear cns config stats
```

Related Commands

Command	Description
show cns config stats	Displays statistics about the CNS configuration agent.

clear cns counters

To clear all CNS statistics, use the **clear cns counters** command in privileged EXEC mode.

clear cns counters

Syntax Description

This command has no arguments or keywords.

Defaults

No statistics are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

The **clear cns counters** command clears all the statistics tracked and displayed by CNS agents.

Examples

The following example shows how to clear all of the statistics used by CNS:

```
Router# clear cns counters
```

Related Commands

Command	Description
show cns config stats	Displays statistics about the CNS configuration agent.
show cns event stats	Displays statistics about the CNS event agent.
show cns image stats	Displays statistics about the CNS image agent.

clear cns event stats

To clear the statistics about the CNS event agent, use the **clear cns event stats** command in privileged EXEC mode.

clear cns event stats

Syntax Description

This command has no arguments or keywords.

Defaults

No statistics are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

The **clear cns event stats** command clears all the statistics displayed by the **show cns event stats** command.

Examples

The following example shows how to clear all of the statistics for the CNS event agent:

```
Router# clear cns event stats
```

Related Commands

Command	Description
show cns event stats	Displays statistics about the CNS event agent.

clear cns image connections

To clear the CNS image agent connections statistics, use the **clear cns image connections** command in privileged EXEC mode.

clear cns image connections

Syntax Description

This command has no arguments or keywords.

Defaults

No statistics are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

The **clear cns image connections** command clears all the statistics displayed by the **show cns image connections** command.

Examples

The following example shows how to clear all of the connection statistics for the CNS image agent:

```
Router# clear cns image connections
```

Related Commands

Command	Description
show cns image connections	Displays connection information for the CNS image agent.

clear cns image status

To clear the CNS image agent status statistics, use the **clear cns image status** command in privileged EXEC mode.

clear cns image status

Syntax Description

This command has no arguments or keywords.

Defaults

No statistics are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

The **clear cns image status** command clears all the statistics displayed by the **show cns image status** command.

Examples

The following example shows how to clear all of the status statistics for the CNS image agent:

```
Router# clear cns image status
```

Related Commands

Command	Description
show cns image status	Displays status information for the CNS image agent.

clear logging

To clear messages from the logging buffer, use the **clear logging** command in privileged EXEC mode.

clear logging

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.

Examples

In the following example, the logging buffer is cleared:

```
Router# clear logging

Clear logging buffer [confirm]
Router#
```

Related Commands

Command	Description
logging buffered	Logs messages to an internal buffer.
show logging	Displays the state of logging (syslog).

clear logging xml

To clear the contents of the XML system message logging (syslog) buffer, use the **clear logging xml** command in User EXEC or Priviledged EXEC mode..

clear logging xml

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

This command clears the contents of the XML-formatted logging buffer, but does not clear the contents of the standard logging buffer. The system will prompt you to confirm the action before clearing the buffer.

Examples

In the following example, the XML-specific buffer is cleared:

```
Router# clear logging xml
Clear XML logging buffer [confirm]?y
```

Related Commands

Command	Description
logging buffered xml	Enables system message logging (syslog) to the XML-specific buffer in XML format.
show logging xml	Displays the state of XML-formatted system message logging, followed by the contents of the XML-specific buffer.

clear parser cache

To clear the parse cache entries and hit/miss statistics stored for the Parser Cache feature, use the **clear parser cache** command in privileged EXEC mode.

clear parser cache

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

The Parser Cache feature optimizes the parsing (translation and execution) of Cisco IOS software configuration command lines by remembering how to parse recently encountered command lines, decreasing the time required to process large configuration files.

The **clear parser cache** command will free the system memory used by the Parser Cache feature and will erase the hit/miss statistics stored for the output of the **show parser statistics** EXEC command. This command is only effective when the Parser Cache feature is enabled.

Examples

The following example shows the clearing of the parser cache:

```
Router# show parser statistics

Last configuration file parsed:Number of Commands:1484, Time:820 ms

Parser cache:enabled, 1460 hits, 26 misses
Router# clear parser cache
Router# show parser statistics
Last configuration file parsed:Number of Commands:1484, Time:820 ms

Parser cache:enabled, 0 hits, 1 misses
```

Related Commands

Command	Description
parser cache	Enables or disables the Parser Cache feature.
show parser statistics	Displays statistics about the last configuration file parsed and the status of the Parser Cache feature.

clear saa apm cache

To delete files from the SAA Application Performance Monitor (APM) cache, use the **clear saa apm cache** command in global configuration mode.

clear saa apm cache {**local** | **remote** | **file** *filename*} [**force**]

Syntax Description

local	Deletes all local files from the APM cache.
remote	Deletes all remote files from the APM cache.
file *filename*	Deletes only the specified file from the APM cache.
force	(Optional) Forces the local, remote, or specified file to be deleted. This keyword is required to delete those files tagged as "sticky."

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

This command will not delete files tagged as "sticky" in the APM cache unless the **force** keyword is used. The sticky bit is set for a file when the file is copied to the router using the **saa apm copy** command. To check if files have the sticky bit set, use the **show saa apm cache** command; those files that show a value of 1 in the "SBit" column have the sticky bit enabled, while those with a sticky value of 0 do not have the sticky bit enabled.

Examples

In the following example, all files that are not tagged as "sticky" (as seen in the SBit column of the **show saa apm cache** output) are deleted from the APM cache:

```
Router# show saa apm cache

Cache Size (bytes):100000
Cache used (bytes):2056

   TimeCreated   TimeAccessed   Size Ref Loc Type SBit FileName
09/21 13:31:25 09/21 13:31:48   1170   0   1  SCR    0 user/scripts/ldap-rem.scr
09/21 13:31:20 09/21 13:31:27   1513   0   1  SCR    1 user/scripts/ldap.scr
09/20 14:29:13 09/20 14:29:36    735   0   1  SCR    0 user/scripts/udp-rem.scr

Router# configure terminal
Router(config)# clear saa apm cache local
Router(config)# end
Router# show saa apm cache

Cache Size (bytes):100000
```

```
Cache used (bytes):1513

   TimeCreated   TimeAccessed   Size Ref Loc Type SBit FileName
09/21 13:31:20 09/21 13:31:27   1513   0   1  SCR    1 user/scripts/ldap.scr
```

Related Commands

Command	Description
show saa apm cache	Displays the amount of memory available in the SAA APM cache and information about the files stored in the cache.

clear tcp

To clear a TCP connection, use the **clear tcp** command in privileged EXEC mode.

clear tcp {**line** *line-number* | **local** *hostname port* **remote** *hostname port* | **tcb** *address*}

Syntax Description

line *line-number*	Line number of the TCP connection to clear.
local *hostname port* **remote** *hostname port*	Host name of the local router and port and host name of the remote router and port of the TCP connection to clear.
tcb *address*	Transmission Control Block (TCB) address of the TCP connection to clear. The TCB address is an internal identifier for the endpoint.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

The **clear tcp** command is particularly useful for clearing hung TCP connections.

The **clear tcp line** *line-number* command terminates the TCP connection on the specified tty line. Additionally, all TCP sessions initiated from that tty line are terminated.

The **clear tcp local** *hostname port* **remote** *hostname port* command terminates the specific TCP connection identified by the host name and port pair of the local and remote router.

The **clear tcp tcb** *address* command terminates the specific TCP connection identified by the TCB address.

Examples

The following example clears a TCP connection using its tty line number. The **show tcp** command displays the line number (tty2) that is used in the **clear tcp** command.

```
Router# show tcp

    tty2, virtual tty from host router20.cisco.com
    Connection state is ESTAB, I/O status: 1, unread input bytes: 0
    Local host: 171.69.233.7, Local port: 23
    Foreign host: 171.69.61.75, Foreign port: 1058

    Enqueued packets for retransmit: 0, input: 0, saved: 0

    Event Timers (current time is 0x36144):
    Timer          Starts    Wakeups            Next
    Retrans             4          0             0x0
    TimeWait            0          0             0x0
    AckHold             7          4             0x0
    SendWnd             0          0             0x0
    KeepAlive           0          0             0x0
    GiveUp              0          0             0x0
    PmtuAger            0          0             0x0
```

```
    iss: 4151109680  snduna: 4151109752  sndnxt: 4151109752     sndwnd:  24576
    irs: 1249472001  rcvnxt: 1249472032  rcvwnd:       4258  delrcvwnd:     30

    SRTT: 710 ms, RTTO: 4442 ms, RTV: 1511 ms, KRTT: 0 ms
    minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 300 ms

Router# clear tcp line 2
    [confirm]
     [OK]
```

The following example clears a TCP connection by specifying its local router host name and port and its remote router host name and port. The **show tcp brief** command displays the local (Local Address) and remote (Foreign Address) host names and ports to use in the **clear tcp** command.

```
Router# show tcp brief

TCB       Local Address           Foreign Address        (state)
    60A34E9C  router1.cisco.com.23      router20.cisco.1055  ESTAB

Router# clear tcp local router1 23 remote router20 1055
    [confirm]
     [OK]
```

The following example clears a TCP connection using its TCB address. The **show tcp brief** command displays the TCB address to use in the **clear tcp** command.

```
Router# show tcp brief

    TCB       Local Address           Foreign Address        (state)
    60B75E48  router1.cisco.com.23      router20.cisco.1054  ESTAB

Router# clear tcp tcb 60B75E48
    [confirm]
     [OK]
```

Related Commands

Command	Description
show tcp	Displays the status of TCP connections.
show tcp brief	Displays a concise description of TCP connection endpoints.

clear xsm

To clear XML Subscription Manager (XSM) client sessions, use the **clear xsm** command in privileged EXEC mode.

clear xsm [**session** *number*]

Syntax Description

session *number*	(Optional) XSM session ID number of the specific XSM client session you wish to clear.

Defaults

If the optional **session** *number* syntax is not used, the **clear xsm** command clears all XSM client sessions.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

This command disconnects all active client sessions (such as with a VPN Device Manager [VDM]) on the XSM server, unless you state a specific session number. This command allows troubleshooting of the XSM server and its active clients by allowing individual clients to be disconnected. Use the **show xsm status** command to obtain specific session numbers.

Examples

In the following example, all XSM client sessions are cleared:

```
Router# clear xsm
```

In the following example, XSM client session 10 is cleared:

```
Router# clear xsm session 10
```

Related Commands

Command	Description
show xsm status	Displays information and status about clients subscribed to the XSM server.
xsm	Enables XSM client access to the router.

cli

To specify EXEC command line interface (CLI) commands within a Command Scheduler policy list, use the **cli** command in kron-policy configuration mode. To delete a CLI command from the current policy list, use the **no** form of this command.

cli *command*

no cli *command*

Syntax Description

command	EXEC mode CLI command syntax. Commands must not generate a prompt or allow interruption by any keystroke.

Defaults

No CLI commands are specified.

Command Modes

Kron-policy configuration (config-kron-policy)

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use the **cli** command in conjunction with the **kron policy-list** command to create a policy list containing EXEC CLI commands to be scheduled to run on the router at a specified time. Use the **kron occurrence** and **policy-list** commands to schedule one or more policy lists to run at the same time or interval.

The Command Scheduler process is useful to automate the running of EXEC commands at recurring intervals, and it can be used in remote routers to minimize manual intervention.

Examples

The following example shows how to configure the EXEC command **cns image retrieve** within the policy list named three-day-list:

```
Router(config)# kron policy-list three-day-list
Router(config-kron-policy)# cli cns image retrieve server https://10.19.2.3/cns/image/
status https://10.19.2.3/cnsstatus/imageinfo/
```

Related Commands

Command	Description
kron occurrence	Specifies schedule parameters for a Command Scheduler occurrence and enters kron-occurrence configuration mode.
kron policy-list	Specifies a name for a Command Scheduler policy and enters kron-policy configuration mode.
policy-list	Specifies the policy list associated with a Command Scheduler occurrence.

cli (cns)

To specify the command lines of a Cisco Networking Services (CNS) connect template, use the **cli** command in CNS template connect configuration mode. To disable this configuration, use the **no** form of this command.

cli *config-text*

no cli *config-text*

Syntax Description

config-text	Command line to be included in a CNS connect template.

Defaults

No command lines are specified in the CNS connect template.

Command Modes

CNS template connect configuration

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.3(9)	This command was integrated into Cisco IOS Release 12.3(9). The CNS connect variable **${dlci}** is not supported in this release.

Usage Guidelines

First use the **cns template connect** command to enter CNS template connect configuration mode and define the name of the CNS connect template to be configured. Then use the **cli** command to specify the command lines of the CNS connect template.

Note Effective with Cisco IOS Releases 12.3(8)T and 12.3(9), the **config-cli** and **line-cli** commands are replaced by the **cli (cns)** command.

The command lines specified using the **cli** command can include CNS connect variables (see Table 12). These variables act as placeholders within the command lines of a CNS connect template. Each variable is defined by an associated **discover** command. Before a CNS connect template that contains these variables is applied to a router's configuration, the variables are replaced by the values defined by their associated **discover** command. For example, if the **discover interface serial** command was configured, and you were able to connect to the CNS configuration engine using Serial0/0, then the **cli ip route 0.0.0.0 0.0.0.0 ${interface}** command would generate the **cli ip route 0.0.0.0 0.0.0.0 serial0/0** command.

Note When creating a CNS connect template, you must enter the **exit** command to complete the configuration of the template and exit from CNS template connect configuration mode. This requirement was implemented to prevent accidentally entering a command without the **cli** command.

Table 12 Summary of the CNS Connect Variables

Variable	Description
${line}	The line type defined by the associated **discover line** *line-type* command.
${controller}	The controller type defined by the associated **discover controller** *controller-type* command.
${interface}	The interface type defined by the associated **discover interface** command.
${dlci}	The active DLCI defined by the associated **discover dlci** command.
${next-hop}	The next hop interface. This variable is identical to the **${interface}** variable unless the **discover dlci** command has been configured. In this case, the **${next-hop}** variable is identical to the **${interface}.{subinterface}** variable, where the **{subinterface}** variable is specified by the **discover dlci** command. The **${next-hop}** variable should only be used in the CNS connect templates after the last **discover** command has been entered. A typical use of this variable is to allow the default IP route to be configured to send traffic towards the CNS configuration engine. Note that the CNS configuration engine may not be on the same LAN as the router. Therefore, configuring a route to the CNS configuration engine may require deployment-specific knowledge. Common practice is to define a default route to the interface using the **ip route** command (for example, **cli ip route 0.0.0.0 0.0.0.0 ${next-hop}**).
$$	A literal substitution of the $ symbol.

Note Effective with Cisco IOS Releases 12.3(8)T and 12.3(9), the **&** variable is replaced by the **${interface}** variable.

Examples

The following example shows how to configure a CNS connect template named template1:

```
Router (config)# cns template connect template-1
Router (config-templ-conn)# cli command-1
Router (config-templ-conn)# cli command-2
Router (config-templ-conn)# cli no command-3
Router (config-templ-conn)# exit
Router (config)#
```

When the template1 template is applied, the following commands are sent to the router's parser:

```
command-1
command-2
no command-3
```

When the template1 template is removed from the router's configuration after an unsuccessful ping attempt to the CNS configuration engine, the following commands are sent to the router's parser:

```
no command-1
no command-2
command-3
```

Related Commands

Command	Description
cns connect	Enters CNS connect configuration mode and defines the parameters of a CNS connect profile for connecting to the CNS configuration engine.
cns template connect	Enters CNS template connect configuration mode and defines the name of a CNS connect template.
discover (cns)	Defines the interface parameters within a CNS connect profile for connecting to the CNS configuration engine.
template (cns)	Specifies a list of CNS connect templates within a CNS connect profile to be applied to a router's configuration.

clock calendar-valid

To configure a system as an authoritative time source for a network based on its hardware clock (calendar), use the **clock calendar-valid** command in global configuration mode. To specify that the hardware clock is not an authoritative time source, use the **no** form of this command.

clock calendar-valid

no clock calendar-valid

Syntax Description

This command has no arguments or keywords.

Defaults

The router is not configured as a time source.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Some platforms have a hardware clock that is separate from the software clock. The hardware clock runs continuously, even if the router is powered off or rebooted. If no outside time source is available on your network, use this command to make the hardware clock an authoritative time source.

Because the hardware clock is not as accurate as other time sources, you should configure this command only when a more accurate time source (such as NTP) is not available.

Examples

The following example configures a router as the time source for a network based on its hardware clock:

```
Router(config)# clock calendar-valid
```

Related Commands

Command	Description
ntp master	Configures the Cisco IOS software as an NTP master clock to which peers synchronize themselves when an external NTP source is not available.
vines time use-system	Sets VINES network time based on the system time.

clock read-calendar

To manually read the hardware clock (calendar) settings into the software clock, use the **clock read-calendar** command in EXEC mode.

clock read-calendar

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Some platforms have a hardware clock that is separate from the software clock. The hardware clock runs continuously, even if the router is powered off or rebooted. When the router is rebooted, the hardware clock is automatically read into the software clock. However, you may use this command to manually read the hardware clock setting into the software clock. This command is useful if the **calendar set** command has been used to change the setting of the hardware clock.

Examples

The following example configures the software clock to set its date and time by the hardware clock setting:

```
Router> clock read-calendar
```

Related Commands

Command	Description
calendar set	Sets the hardware clock.
clock set	Manually sets the software clock.
clock update-calendar	Performs a one-time update of the hardware clock from the software clock.
ntp update-calendar	Periodically updates the hardware clock from the software clock.

clock set

To manually set the system software clock, use one of the following formats of the **clock set** command in Privileged EXEC mode.

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

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

Syntax Description

hh:*mm*:*ss*	Current time in hours (24-hour format), minutes, and seconds.
day	Current day (by date) in the month.
month	Current month (by name).
year	Current year (no abbreviation).

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Generally, if the system is synchronized by a valid outside timing mechanism, such as a Network Time Protocol (NTP) or VINES clock source, or if you have a router with hardware clock, you need not set the software clock. Use this command if no other time sources are available. The time specified in this command is assumed to be in the timezone specified by the configuration of the **clock timezone** command.

Examples

The following example manually sets the software clock to 7:29 p.m. on May 13, 2003:

```
Router# clock set 19:29:00 13 May 2003
```

Related Commands

Command	Description
calendar set	Sets the hardware clock.
clock read-calendar	Performs a one-time update of the software clock from the hardware clock (calendar).
clock summer-time	Configures the system to automatically switch to summer time (daylight saving time).
clock timezone	Sets the time zone for display purposes.

clock summer-time

To configure the system to automatically switch to summer time (daylight saving time), use one of the formats of the **clock summer-time** command in global configuration mode. To configure the Cisco IOS software not to automatically switch to summer time, use the **no** form of this command.

clock summer-time *zone* **recurring** [*week day month hh*:*mm week day month hh*:*mm* [*offset*]]

clock summer-time *zone* **date** *date month year hh*:*mm date month year hh*:*mm* [*offset*]

clock summer-time *zone* **date** *month date year hh*:*mm month date year hh*:*mm* [*offset*]

no clock summer-time

Syntax Description

zone	Name of the time zone (for example, "PDT" for Pacific Daylight Time) to be displayed when summer time is in effect. The length of the *zone* argument is limited to 7 characters.
recurring	Indicates that summer time should start and end on the corresponding specified days every year.
date	Indicates that summer time should start on the first specific date listed in the command and end on the second specific date in the command.
week	(Optional) Week of the month (1 to 5 or **last**).
day	(Optional) Day of the week (Sunday, Monday, and so on).
date	Date of the month (1 to 31).
month	(Optional) Month (January, February, and so on).
year	Year (1993 to 2035).
hh:*mm*	(Optional) Time (military format) in hours and minutes.
offset	(Optional) Number of minutes to add during summer time (default is 60).

Defaults

Summer time is disabled. If the **clock summer-time** *zone* **recurring** command is specified without parameters, the summer time rules default to United States rules. Default of the *offset* argument is 60.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command if you want to automatically switch to summer time (for display purposes only). Use the **recurring** form of the command if the local summer time rules are of this form. Use the **date** keyword to specify a start and end date for summer time if you cannot use the **recurring** keyword.

In both the **date** and **recurring** forms of the command, the first part of the command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is chronologically after the ending month, the system assumes that you are in the southern hemisphere.

Examples

The following example specifies that summer time starts on the first Sunday in April at 2 a.m. and ends on the last Sunday in October at 2 a.m.:

```
Router(config)# clock summer-time PDT recurring 1 Sunday April 2:00 last Sunday October
2:00
```

If you live in a place where summer time does not follow the pattern in the first example, you can specify the exact date and times. In the following example, daylight saving time (summer time) is configured to start on October 12, 1997 at 2 a.m., and end on April 26, 1998 at 2 a.m.:

```
Router(config)# clock summer-time date 12 October 1997 2:00 26 April 1998 2:00
```

Related Commands

Command	Description
calendar set	Sets the hardware clock.
clock timezone	Sets the time zone for display purposes.

clock timezone

To set the time zone for display purposes, use the **clock timezone** command in global configuration mode. To set the time to Coordinated Universal Time (UTC), use the **no** form of this command.

clock timezone *zone hours-offset* [*minutes-offset*]

no clock timezone

Syntax Description

zone	Name of the time zone to be displayed when standard time is in effect. The length of the *zone* argument is limited to 7 characters.
hours-offset	Hours difference from UTC.
minutes-offset	(Optional) Minutes difference from UTC.

Defaults

UTC

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The system internally keeps time in UTC, so this command is used only for display purposes and when the time is manually set.

Table 13 lists common time zone acronyms used for the *zone* argument.

Table 13 Common Time Zone Acronyms

Acronym	Time Zone Name and UTC Offset
Europe	
GMT	Greenwich Mean Time, as UTC
BST	British Summer Time, as UTC + 1 hour
IST	Irish Summer Time, as UTC + 1 hour
WET	Western Europe Time, as UTC
WEST	Western Europe Summer Time, as UTC + 1 hour
CET	Central Europe Time, as UTC + 1
CEST	Central Europe Summer Time, as UTC + 2
EET	Eastern Europe Time, as UTC + 2
EEST	Eastern Europe Summer Time, as UTC + 3
MSK	Moscow Time, as UTC + 3

Table 13 Common Time Zone Acronyms (continued)

Acronym	Time Zone Name and UTC Offset
MSD	Moscow Summer Time, as UTC + 4
United States and Canada	
AST	Atlantic Standard Time, as UTC –4 hours
ADT	Atlantic Daylight Time, as UTC –3 hours
ET	Eastern Time, either as EST or EDT, depending on place and time of year
EST	Eastern Standard Time, as UTC –5 hours
EDT	Eastern Daylight Saving Time, as UTC –4 hours
CT	Central Time, either as CST or CDT, depending on place and time of year
CST	Central Standard Time, as UTC –6 hours
CDT	Central Daylight Saving Time, as UTC –5 hours
MT	Mountain Time, either as MST or MDT, depending on place and time of year
MST	Mountain Standard Time, as UTC –7 hours
MDT	Mountain Daylight Saving Time, as UTC –6 hours
PT	Pacific Time, either as PST or PDT, depending on place and time of year
PST	Pacific Standard Time, as UTC –8 hours
PDT	Pacific Daylight Saving Time, as UTC –7 hours
AKST	Alaska Standard Time, as UTC –9 hours
AKDT	Alaska Standard Daylight Saving Time, as UTC –8 hours
HST	Hawaiian Standard Time, as UTC –10 hours
Australia	
WST	Western Standard Time, as UTC + 8 hours
CST	Central Standard Time, as UTC + 9.5 hours
EST	Eastern Standard/Summer Time, as UTC + 10 hours (+11 hours during summer time)

Table 14lists an alternative method for referring to time zones, in which single letters are used to refer to the time zone difference from UTC. Using this method, the letter Z is used to indicate the zero meridian, equivalent to UTC, and the letter J (Juliet) is used to refer to the local time zone. Using this method, the International Date Line is between time zones M and Y.

Table 14 Single-Letter Time Zone Designators

Letter Designator	Word Designator	Difference from UTC
Y	Yankee	UTC –12 hours
X	Xray	UTC –11 hours
W	Whiskey	UTC –10 hours
V	Victor	UTC –9 hours
U	Uniform	UTC –8 hours
T	Tango	UTC –7 hours
S	Sierra	UTC –6 hours
R	Romeo	UTC –5 hours
Q	Quebec	UTC –4 hours
P	Papa	UTC –3 hours
O	Oscar	UTC –2 hours
N	November	UTC –1 hour
Z	Zulu	Same as UTC
A	Alpha	UTC +1 hour
B	Bravo	UTC +2 hours
C	Charlie	UTC +3 hours
D	Delta	UTC +4 hours
E	Echo	UTC +5 hours
F	Foxtrot	UTC +6 hours
G	Golf	UTC +7 hours
H	Hotel	UTC +8 hours
I	India	UTC +9 hours
K	Kilo	UTC +10 hours
L	Lima	UTC +11 hours
M	Mike	UTC +12 hours

The following example sets the time zone to Pacific Standard Time (PST), which is 8 hours behind UTC:

```
Router(config)# clock timezone PST -8
```

The following example sets the time zone to Atlantic Time (AT) for Newfoundland, Canada, which is 3.5 hours behind UTC:

```
Router(config)# clock timezone AT -3 30
```

Related Commands

Command	Description
calendar set	Sets the hardware clock.
clock set	Manually set the software clock.

Command	Description
clock summer-time	Configures the system to automatically switch to summer time (daylight saving time).
show clock	Displays the software clock.

clock update-calendar

To perform a one-time update of the hardware clock (calendar) from the software clock, use the **clock update-calendar** command in user EXEC or privileged EXEC mode.

clock update-calendar

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Some platforms have a hardware clock (calendar) in addition to a software clock. The hardware clock is battery operated, and runs continuously, even if the router is powered off or rebooted.

If the software clock and hardware clock are not synchronized, and the software clock is more accurate, use this command to update the hardware clock to the correct date and time.

Examples

The following example copies the current date and time from the software clock to the hardware clock:

```
Router> clock update-calendar
```

Related Commands

Command	Description
clock read-calendar	Performs a one-time update of the software clock from the hardware clock (calendar).
ntp update-calendar	Periodically updates the hardware clock from the software clock.

cns config cancel

To remove a partial Cisco Networking Services (CNS) configuration from the list of outstanding partial configurations, use the **cns config cancel** command in EXEC mode.

cns config cancel *queue-id*

Syntax Description

queue-id	Indicates which partial configuration in the list of outstanding partial configurations to remove from the list. This list can be displayed by issuing the **show cns config outstanding** command in EXEC mode.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0 ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0 S.
12.2(8)T	This command was implemented on additional platforms.

Usage Guidelines

Incremental (partial) configurations take place in two steps:

1. The configuration agent receives the partial configuration. It checks the configuration commands for syntax, publishes the success or failure of the read and syntax-check operation to the sync-status subject “cisco.cns.config.sync-status,” and stores the configuration.
2. The configuration agent receives a second event message directing it to either apply or cancel the stored configuration.

Use the **cns config cancel** command in error scenarios where the second event message is not received and you need to remove the configuration from the list of outstanding configurations. Currently the maximum number of outstanding configurations is one.

Examples

The following example shows the process of checking the existing outstanding CNS configurations and cancelling the configuration with the *queue-id* of 1:

```
Router# show cns config outstanding
The outstanding configuration information:
queue id   identifier       config-id
1          identifierREAD   config_idREAD

Router# cns config cancel 1
```

```
Router# show cns config outstanding
The outstanding configuration information:
queue id   identifier       config-id
```

Related Commands

Command	Description
cns config partial	Starts the CNS configuration agent, which provides CNS configuration services to Cisco IOS clients.
cns event	Configures the CNS event gateway, which provides CNS event services to Cisco IOS clients.
show cns event connections	Displays the status of the CNS event agent connection.
show cns config outstanding	Displays information about incremental CNS configurations that have started but not yet completed.

cns config connect-intf

Note Effective with Cisco IOS Releases 12.3(8)T and 12.3(9), the **cns config connect-intf** command is replaced by the **cns connect** and **cns template connect** commands. See the **cns connect** and **cns template connect** commands for more information.

To specify the interface for connecting to the Cisco Networking Services (CNS) configuration engine, use the **cns config connect-intf** command in global configuration mode. To disable this interface for the connection, use the **no** form of this command.

cns config connect-intf *type number* [**ping-interval** *seconds*] [**retries** *number*]

no cns config connect-intf *type number*

Syntax Description

type number	Interface type and number for the connecting interface.
ping-interval *seconds*	(Optional) Interval between successive ping attempts. Values are from 1 to 30 seconds. The default is 10 seconds.
retries *number*	(Optional) Number of times that a ping will be retried. Values are from 1 to 30 seconds. The default is 5 seconds.

Defaults

The ping interval defaults to 10 seconds.

The number of retries defaults to 5.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.3(8)T	This command was replaced by the **cns connect** and **cns template connect** commands.
12.3(9)	This command was replaced by the **cns connect** and **cns template connect** commands.

Usage Guidelines

Use this command to connect to the CNS configuration engine using a specific type of interface. You must specify the interface type but need not specify the interface number; the router's bootstrap configuration finds the connecting interface, regardless of the slot in which the card resides or the modem dialout line for the connection, by trying different candidate interfaces or lines until it successfully pings the registrar.

Use this command to enter CSN Connect-interface configuration mode (config-cns-conn-if). Then use one of the following bootstrap-configuration commands to connect to the registrar for initial configuration:

- **config-cli** followed by commands that, used as is, configure the interface.
- **line-cli** followed by a command to configure modem lines to enable dialout and, after that, commands to configure the modem dialout line.

The **config-cli** command accepts the special directive character "**&**," which acts as a placeholder for the interface name. When the configuration is applied, the **&** is replaced with the interface name. Thus, for example, if we are able to connect using FastEthernet0/0, the **config-cli ip route 0.0.0.0 0.0.0.0 &** command generates the **ip route 0.0.0.0 0.0.0.0 FastEthernet0/0** command. Similarly, the **config-virtual terminal line (vty) cns id & ipaddress** command generates the **cns id FastEthernet0/0 ipaddress** command.

Examples

In the following example, the user connects to a configuration engine using the asynchronous interface and issues a number of commands:

```
Router(config)# cns config connect-intf Async
Router(config-cns-conn-if)# config-cli encapsulation ppp
Router(config-cns-conn-if)# config-cli ip unnumbered FastEthernet0/0
Router(config-cns-conn-if)# config-cli dialer rotary-group 0
Router(config-cns-conn-if)# line-cli modem InOut
Router(config-cns-conn-if)# line-cli
.
.
.
Router(config-cns-conn-if)# exit
```

These commands result in the following configuration being applied:

```
line 65
modem InOut
.
.
.
interface Async65
encapsulation ppp
dialer in-band
dialer rotary-group 0
```

Related Commands

Command	Description
cns config cancel	Cancels an incremental two-phase synchronization configuration.
cns config initial	Starts the CNS configuration agent and initiates an initial configuration.
cns config notify	Detects CNS configuration changes and sends an event containing the previous and current configuration.
cns config partial	Starts the CNS configuration agent, which provides CNS configuration services to Cisco IOS clients.

cns config initial

To enable the CNS configuration agent and initiate a download of the initial configuration, use the **cns config initial** command in global configuration mode. To remove an existing **cns config initial** command from the running configuration of the routing device, use the **no** form of this command.

cns config initial {*ip-address* | *host-name*} [**encrypt**] [*port-number*] [**page** *page*] [**syntax-check**] [**no-persist**] [**source** *ip-address*] [**event**] [**inventory**]

no cns config initial

Syntax Description

ip-address	IP address of the configuration server.
host-name	Host name of the configuration server.
encrypt	(Optional) Uses a Secure Socket Layer (SSL) encrypted link to the event gateway.
port-number	(Optional) Port number of the configuration service. The value is from 0 to 65535. The default is 80 with no encryption and 443 with encryption.
page *page*	(Optional) Web page where the configuration is located. The default is /cns/config.asp.
syntax-check	(Optional) Turns on syntax checking.
no-persist	(Optional) Suppresses the default automatic writing to NVRAM of the configuration pulled as a result of issuing the **cns config initial** command. If not present, issuing the **cns config initial** command causes the resultant configuration to be automatically written to NVRAM.
source *ip-address*	(Optional) IP address to use as the source of CNS communications.
event	(Optional) Sends an event to the Event Bus notifying successful completion of the configuration or warning that the configuration contained errors. If the CNS event agent is not configured, the event will be saved until the CNS event agent is enabled. If the **event** keyword is not specified, a log message is sent to the console of the device after the configuration is complete.
inventory	(Optional) Sends an inventory of the line cards and modules in the router to the CNS configuration engine as part of the HTTP request.

Defaults

The port number defaults to 80 with no encryption and 443 with encryption.
Default web page of the initial configuration is /cns/config.asp.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.

Release	Modification
12.2(2)XB	This command was implemented on Cisco IAD2420 series Integrated Access Devices (IADs).
12.2(8)T	The **source** and **encrypt** keywords were added.
12.3(1)	The **inventory** keyword was added.

Usage Guidelines

Use this command when a basic configuration—called a bootstrap configuration—is added to multiple routers before being deployed. When a router is initially powered (or each time a router is reloaded when the **no-persist** keyword is used) the **cns config initial** command will cause a configuration file—called an initial configuration—for the router to be downloaded from the configuration server. The initial configuration can be unique for each router.

When the configuration has been received by the router, each line of the configuration will be applied in the same order as it was received. If the Cisco IOS parser has an error with one of the lines of the configuration, then all the configuration up to this point will be applied to the router, but none of the configuration beyond the error will be applied. If an error occurs, the command will retry until it successfully completes. Once the configuration has successfully completed the **cns config initial** command will be removed from the running configuration. By default, NVRAM will be updated except when the **no-persist** keyword is configured.

When this command is used with the **event** keyword, a single message will be published on the event bus after the configuration is complete. The event bus will display one of the following status messages:

- cisco.mgmt.cns.config.complete—CNS configuration agent successfully applied the initial configuration.
- cisco.mgmt.cns.config.warning—CNS configuration agent fully applied the initial configuration, but encountered possible semantic errors.

Examples

The following example shows how to enable the CNS configuration agent and initiate an initial configuration:

```
Router# cns config initial 10.19.4.5 page /cns/config/first.asp
```

Related Commands

Command	Description
cns config connect-intf	Specifies the interface for connecting to the CNS configuration engine.
cns config notify	Detects CNS configuration changes and sends an event containing the previous and current configuration.
cns config retrieve	Returns the configuration of a routing device if the CNS configuration agent is enabled and the partial configuration is complete.
cns event	Configures the CNS event gateway, which provides CNS event services to Cisco IOS clients.
show cns config status	Displays information about the status of the CNS configuration agent.

cns config notify

To notify CNS agents of configuration changes on Cisco IOS devices, use the **cns config notify** command in global configuration mode. To disable notifications, use the **no** form of this command.

cns config notify {**all** | **diff**} [**interval** *minutes*] [**no_cns_events**] [**old-format**]

no cns config notify {**all** | **diff**} [**interval** *minutes*] [**no-cns-events**] [**old-format**]

Syntax Description

all	Captures all configuration commands for the config-changed event output.
diff	Captures commands that change configuration for the config-changed event output.
interval *minutes*	(Optional) Specifies the amount of time after the last configuration change that the config-changed event is sent. The default is 5 minutes. The timer starts when you make a configuration change and you remain in configuration mode after the configuration change. If you enter the **end** command, the config-changed event is sent immediately.
no_cns_events	(Optional) Disables event notification for configurations changed through an XML file. If the configuration is changed using the command-line interface (CLI), the config-changed event will be sent.
old-format	(Optional) Provides the event notification in the old XML format for backwards compatibility.

Defaults

The interval defaults to 5 minutes.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(11)T	The **diff** keyword was removed.
12.3(1)	The **diff** and **old-format** keywords were added.

Usage Guidelines

When the **cns config notify** command is enabled, commands entered in configuration mode are detected. If the **all** keyword is specified, the command is stored for future notification. If the **diff** keyword is specified, the command is stored for future notification if the software determines that the command will cause a configuration change. The **diff** keyword also allows the software to store information about the command including previous configuration states, source of the change (for example, a telnet user), and the time of configuration.

The stored information is formatted in XML and sent as part of a CNS config agent change notification event. A CNS config agent change notification event is sent to the CNS Event Bus when configuration mode is exited or no activity from that source has occurred for the configured interval time.

You must enable the CNS event agent using the **cns event** command before configuring this command. If the CNS event agent is not configured, the notification event will be queued and sent when the CNS event agent is enabled. If the CNS config notify queue is full, subsequent events are dropped and a "lost" CNS config change notification is sent when the CNS event agent is enabled.

Use the **no_cns_events** for applications that already record configuration changes sent to the routing device through the CNS Event Bus.

Use the **old-format** keyword to generate XML output—only the entered command and previous configuration state—that is compatible with the versions of this commands when the **diff** keyword was removed.

Examples

The following example detects configuration changes for all configuration commands:

```
Router(config)# cns config notify all
```

Related Commands

Command	Description
cns config cancel	Cancels an incremental two-phase synchronization configuration.
cns config connect-intf	Specifies the interface for connecting to the CNS configuration engine.
cns config initial	Starts the CNS configuration agent and initiates an initial configuration.
cns config partial	Starts the CNS configuration agent, which provides CNS configuration services to Cisco IOS clients.
cns event	Enables and configures CNS event agent services.

cns config partial

To start the CNS configuration agent and accept a partial configuration, use the **cns config partial** command in global configuration mode. To shut down the CNS partial configuration agent, use the **no** form of this command.

cns config partial {*ip-address* | *host-name*} [**encrypt**] [*port-number*] [**source** *ip-address*] [**inventory**]

no cns config partial

Syntax Description

ip-address	IP address of the configuration server.
host-name	Host name of the configuration server.
encrypt	(Optional) Uses a Secure Socket Layer (SSL) encrypted link between the router and the web server.
port-number	(Optional) Port number of the configuration service. The value is from 0 to 65535. The default is 80 with no encryption and 443 with encryption.
source *ip-address*	(Optional) IP address to use for source of this device.
inventory	(Optional) Sends an inventory of the line cards and modules in the router to the CNS configuration engine as part of the HTTP request.

Defaults

The port number defaults to 80 with no encryption and 443 with encryption.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(2)XB	This command was implemented on Cisco IAD2420 series Integrated Access Devices (IADs).
12.2(8)T	The **source** and **encrypt** keywords were added.
12.3(1)	The **inventory** keyword was added.

Usage Guidelines

Use this command to start the CNS partial configuration agent. You must enable the CNS event agent using the **cns event** command before configuring this command. The CNS event agent sends an event with the subject “cisco.mgmt.cns.config.load” to specify whether configuration data can be pushed to the CNS partial configuration agent or pulled from a configuration server by the CNS partial configuration agent.

In the push model, the event message delivers the configuration data to the partial configuration agent.

In the pull model, the event message triggers the partial configuration agent to pull the configuration data from the CNS configuration engine. The event message contains information about the CNS configuration engine, not the actual configuration data. The host name or IP address is the address of the CNS configuration engine from which the configuration is pulled. Use the **cns trusted-server** command to specify which CNS configuration engines can be used by the CNS partial configuration agent.

When the configuration has been received by the router, each line of the configuration will be applied in the same order as it was received. If the IOS parser has an error with one of the lines of the configuration, then all the configuration up to this point will be applied to the router, but none of the configuration beyond the error will be applied. If an error occurs, the command will retry until it successfully completes. In the pull mode, the command will not retry after an error. By default, NVRAM will be updated except when the **no-persist** keyword is configured.

A single message will be published on the CNS Event Bus after the partial configuration is complete. The CNS Event Bus will display one of the following status messages:

- cisco.mgmt.cns.config.complete—CNS configuration agent successfully applied the partial configuration.
- cisco.mgmt.cns.config.warning—CNS configuration agent fully applied the partial configuration, but encountered possible semantic errors.
- cisco.mgmt.cns.config.failure—CNS configuration agent encountered an error and was not able to apply the configuration.

Examples

The following example shows how to configure the CNS partial configuration agent to accept events from the event gateway at 172.28.129.22. The CNS partial configuration agent will connect to the CNS configuration server at 172.28.129.22, port number 80. The CNS partial configuration agent requests are redirected to a configuration server at 172.28.129.40, port number 80.

```
Router(config)# cns event 172.28.129.22
Router(config)# cns trusted-server config 172.28.129.40
Router(config)# cns config partial 172.28.129.22
```

Related Commands

Command	Description
cns config initial	Starts the CNS configuration agent and initiates an initial configuration.
cns event	Enables and configures CNS event agent services.
cns trusted-server	Specifies a trusted server for CNS agents.
show cns config outstanding	Displays information about incremental CNS configurations that have started but are not yet completed.

cns config retrieve

To request the configuration of a routing device, use the **cns config retrieve** command in EXEC mode.

cns config retrieve {*ip-address* | *host-name*} [**encrypt**] [*port-number*] [**page** *page*] [**overwrite-startup**] [**syntax-check**] [**no-persist**] [**source** *ip-address*] [**event**] [**inventory**]

Syntax Description

ip-address	IP address of the configuration server.
host-name	Host name of the configuration server.
encrypt	(Optional) Uses a Secure Socket Layer (SSL) encrypted link to the event gateway.
port-number	(Optional) Port number of the configuration service. The value is from 0 to 65535. The default is 80 with no encryption and 443 with encryption.
page *page*	(Optional) Web page where the configuration is located. The default is /cns/config.asp.
overwrite-startup	(Optional) Replaces the startup configuration file. Does not apply to the running configuration file.
syntax-check	(Optional) Turns on syntax checking.
no-persist	(Optional) Suppresses the default automatic writing to NVRAM of the configuration pulled as a result of issuing the **cns config retrieve** command. If not present, issuing the **cns config retrieve** command causes the resultant configuration to be automatically written to NVRAM.
source *ip-address*	(Optional) IP address to use as the source of CNS communications.
event	(Optional) Sends an event to the CNS Event Bus stating successful completion of the configuration, a warning that the configuration contained errors, or a message noting that the configuration failed. If the CNS event agent is not configured, the event will be saved until the CNS event agent is enabled. If the **event** keyword is not specified, a log message is sent to the console of the device after the configuration is complete.
inventory	(Optional) Sends an inventory of the line cards and modules in the router to the CNS configuration engine as part of the HTTP request.

Defaults

The port number defaults to 80 with no encryption and 443 with encryption.
Default web page of the initial configuration is /cns/config.asp.

Command Modes

EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.3(1)	The **inventory** keyword was added.

Usage Guidelines

Use this command to request the configuration of a device from a configuration server. Use the **cns trusted-server** command to specify which configuration server can be used (trusted).

When the configuration has been received by the router, each line of the configuration will be applied in the same order as it was received. If the IOS parser has an error with one of the lines of the configuration, then all the configuration up to this point will be applied to the router, but none of the configuration beyond the error will be applied. If an error occurs, the command will not retry.

A single message will be published on the event bus after the partial configuration is complete. The event bus will display one of the following status messages:

- cisco.mgmt.cns.config.complete—CNS configuration agent successfully applied the configuration.
- cisco.mgmt.cns.config.warning—CNS configuration agent fully applied the configuration, but encountered possible semantic errors.
- cisco.mgmt.cns.config.failure—CNS configuration agent encountered an error and was not able to apply the configuration.

The **cns config retrieve** command can be used with Command Scheduler commands (for example, **kron policy-list** and **cli** commands) in environments where it is not practical to use the CNS event agent and the **cns config partial** command. Configured within the **cli** command, the **cns config retrieve** command can be used to poll the configuration server to detect configuration changes.

Examples

The following example shows how to request a configuration from a trusted server at 10.1.1.1:

```
Router(config)# cns trusted-server all 10.1.1.1
Router(config)# cns config retrieve 10.1.1.1
```

Related Commands

Command	Description
cli	Specifies EXEC CLI commands within a Command Scheduler policy list.
cns config initial	Starts the CNS configuration agent and initiates an initial configuration.
cns trusted-server	Specifies a trusted server for CNS agents.
kron policy-list	Specifies a name for a Command Scheduler policy and enters kron-policy configuration mode.
show cns config status	Displays information about the status of the CNS configuration agent.

cns connect

To enter Cisco Networking Services (CNS) connect configuration mode and define the parameters of a CNS connect profile for connecting to the CNS configuration engine, use the **cns connect** command in global configuration mode. To disable the CNS connect profile, use the **no** form of this command.

cns connect *name* [**ping-interval** *interval-seconds*] [**retries** *number-retries*] [**timeout** *timeout-seconds*] [**sleep** *sleep-seconds*]

no cns connect *name* [**ping-interval** *interval-seconds*] [**retries** *number-retries*] [**timeout** *timeout-seconds*] [**sleep** *sleep-seconds*]

Syntax Description

name	The name of the CNS connect profile to be configured.
ping-interval *interval-seconds*	(Optional) Sets the interval (in seconds) between each successive attempt to ping the CNS configuration engine. The default value is 10 seconds.
retries *number-retries*	(Optional) Sets the number of times the CNS connect function will try to ping the CNS configuration engine. The default value is 3.
timeout *timeout-seconds*	(Optional) Sets the amount of time (in seconds) after which an interface is no longer used for ping attempts. The default value is 120 seconds.
sleep *sleep-seconds*	(Optional) Sets the amount of time (in seconds) before which the first ping is attempted for each interface. This option provides time for the far end of a link to stabilize. The default value is 0 seconds.

Defaults

No CNS connect profiles are defined.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.3(9)	This command was integrated into Cisco IOS Release 12.3(9).

Usage Guidelines

Use the **cns connect** command to enter CNS connect configuration mode and define the parameters of a CNS connect profile for connecting to the CNS configuration engine. Then use the following CNS connect commands to create a CNS connect profile:

- **discover**
- **template**

A CNS connect profile specifies the **discover** commands and associated **template** commands that are to be applied to a router's configuration. When multiple **discover** and **template** commands are configured in a CNS connect profile, they are processed in the order in which they are entered.

Note Effective with Cisco IOS Releases 12.3(8)T and 12.3(9), the **cns config connect-intf** command is replaced by the **cns connect** and **cns template connect** commands.

Examples

The following example shows how to create a CNS connect profile named profile-1:

```
Router (config)# cns connect profile-1
Router (config-cns-conn)# discover interface Serial
Router (config-cns-conn)# template template-1
Router (config-cns-conn)# exit
Router (config)#
```

In this example, the following sequence of events occurs for each serial interface when the **cns connect profile-1** command is processed:

1. Enter interface configuration mode and apply all commands in the template-1 template to the router's configuration.
2. Try to ping the CNS configuration engine.
3. If the ping is successful, then download pertinent configuration information from the CNS configuration engine and exit. The **cns connect profile-1** command has completed its process.
4. If the ping is unsuccessful, enter interface configuration mode and remove all commands in the template-1 template from the router's configuration. The **cns connect profile-1** command has failed to retrieve any configuration information from the CNS configuration engine.

Related Commands

Command	Description
cli (cns)	Specifies the command lines of a CNS connect template.
cns template connect	Enters CNS template connect configuration mode and defines the name of a CNS connect template.
discover (cns)	Defines the interface parameters within a CNS connect profile for connecting to the CNS configuration engine.
template (cns)	Specifies a list of CNS connect templates within a CNS connect profile to be applied to a router's configuration.

cns event

To configure the CNS event gateway, which provides CNS event services to Cisco IOS clients, use the **cns event** command in global configuration mode. To remove the specified event gateway from the gateway list, use the **no** form of this command.

cns event {*host-name* | *ip-address*} [*port-number*] [**encrypt**] [**backup**] [**failover-time** *seconds*] [**keepalive** *seconds retry-count*] [**source** *ip-address*]

no cns event {*host-name* | *ip-address*} [*port-number*] [*port-number*] [**encrypt**] [**backup**] [**failover-time** *seconds*] [**keepalive** *seconds retry-count*] [**source** *ip-address*]

Syntax Description

host-name	Host name of the event gateway.
ip-address	IP address of the event gateway.
port-number	(Optional) Port number for the event gateway. The default is 11011 with no encryption or 11012 with encryption.
encrypt	(Optional) Uses a Secure Socket Layer (SSL) encrypted link to the event gateway.
backup	(Optional) Indicates that this is the backup gateway. If omitted, indicates that this is the primary gateway. Before you can configure a backup gateway, you must already have configured a primary gateway. Optional keywords, if omitted, are set as for the primary gateway.
failover-time *seconds*	(Optional) Specifies a time interval in seconds to wait for the primary gateway route after the route to the backup gateway is established. The default is 3.
keepalive *seconds retry-count*	(Optional) Keepalive timeout in seconds and retry count.
source *ip-address*	(Optional) IP address to use as the source for CNS communications.

Defaults

The event gateway port number default is 11011 with no encryption or 11012 with encryption.
The number of seconds to wait for a primary gateway route defaults to 3.
The system uses format 2.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into the Cisco IOS 12.0(18)ST Release.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(2)XB	This command was implemented on Cisco IAD2420 series Integrated Access Devices (IADs).

Release	Modification
12.2(8)T	The **encrypt**, **init-retry**, **source**, and **force-fmt1** keywords were added.
12.3(1)	The **init-retry** keyword was replaced with the **failover-time** keyword. The **force-fmt1** keyword was removed.

Usage Guidelines

The CNS event agent must be enabled before any of the other CNS agents are configured because the CNS event agent provides a transport connection to the CNS Event Bus for all other CNS agents. The other CNS agents use the connection to the CNS Event Bus to send and receive messages. The CNS event agent does not read or modify the messages.

The **failover-time** keyword is useful if you have a backup CNS event gateway configured. If the CNS event agent is trying to connect to the gateway and it discovers that the route to the backup is available before the route to the primary gateway, the *seconds* argument specifies how long the CNS event agent will continue to search for a route to the primary gateway before attempting to link to the backup gateway.

Unless you are using a bandwidth-constrained link, you should set a keepalive timeout and retry count. Doing so allows the management network to recover gracefully should a Cisco IE2100 configuration engine ever fail. Without the keepalive data, such a failure requires manual intervention on every device. The *seconds* multiplied by the *retry-count* determines the length of idle time before the CNS event agent will disconnect and attempt to reconnect to the gateway. We recommend a minimum *retry-count* of two.

If the optional **source** keyword is used, the source IP address might be a secondary IP address of a specific interface to allow a management network to run on top of a production network.

Examples

The following example shows how to set the address of the primary CNS event gateway to the configuration engine software running on IP address 10.1.2.3, port 11011, with a keepalive of 60 seconds and a retry count of 5:

```
Router(config)# cns event 10.1.2.3 11011 keepalive 60 5
```

Related Commands

Command	Description
cns id	Sets the unique event ID or config ID router identifier.
show cns event status	Displays status information about the CNS event agent.

cns exec

To enable and configure the CNS exec agent, which provides CNS exec services to Cisco IOS clients, use the **cns exec** command in global configuration mode. To disable the use of CNS exec agent services, use the **no** form of this command.

cns exec [*host-name* | *ip-address*] [*port-number*] [**encrypt** [*enc-port-number*]] [**source** *ip-address*]

no cns exec {*host-name* | *ip-address*} [*port-number*] [**encrypt** [*enc-port-number*]] [**source** *ip-address*]

Syntax Description

host-name	(Optional) Host name of the exec server.
ip-address	(Optional) IP address of the exec server.
port-number	(Optional) Port number for the exec server. The default is 80.
encrypt	(Optional) Uses a Secure Socket Layer (SSL) encrypted link to the exec agent server.
enc-port-number	(Optional) Port number for the encrypted exec server. The default is 443.
source	(Optional) Specifies the use of an IP address defined by the *ip-address* argument as the source for CNS exec agent communications.
ip-address	(Optional) IP address.

Defaults

The default exec server port number is 80.
The default encrypted exec server port number is 443.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

The CNS exec agent allows a remote application to execute an EXEC mode command-line interface (CLI) command on a Cisco IOS device by sending an event message containing the command. A restricted set of EXEC CLI commands—**show** commands—are supported.

In previous Cisco IOS Releases the CNS exec agent was enabled when the CNS configuration agent was enabled through the **cns config partial** command.

Examples

The following example shows how to enable the CNS exec agent with an IP address of 10.1.2.3 for the exec agent server, a port number of 93, and a source IP address of 172.17.2.2:

```
Router(config)# cns exec 10.1.2.3 93 source 172.17.2.2
```

Related Commands

Command	Description
cns event	Enables and configures CNS event agent services.
show cns event subject	Displays a list of CNS event agent subjects that are subscribed to by applications.

cns id

To set the unique event ID, config ID, or image ID Cisco IOS device identifier used by CNS services, use the **cns id** command in global configuration mode. To set the identifier to the host name of the Cisco IOS device, use the **no** form of this command.

If ID Choice Is IP Address or MAC Address

cns id *type number* {**dns-reverse** | **ipaddress** | **mac-address**} [**event**] [**image**]

no cns id *type number* {**dns-reverse** | **ipaddress** | **mac-address**} [**event**] [**image**]

If ID Choice Is Anything Else

cns id {**hardware-serial** | **hostname** | **string** *string*} [**event**] [**image**]

no cns id {**hardware-serial** | **hostname** | **string** *string*} [**event**] [**image**]

Syntax Description

type number	Type of interface (for example, **ethernet**, **group-async**, **loopback**, or **virtual-template**) and the interface number. Indicates from which interface the IP or MAC address should be retrieved in order to define the unique ID.
dns-reverse	Uses DNS reverse lookup to retrieve the host name of the Cisco IOS device and assign it as the unique ID.
ipaddress	Uses the IP address specified in the *type number* arguments as the unique ID.
mac-address	Uses the MAC address specified in the *type number* arguments as the unique ID.
event	(Optional) Sets this ID to be the event ID value, which is used to identify the Cisco IOS device for CNS event services. If both optional keywords are omitted, the event ID is set to the host name of the Cisco IOS device.
image	(Optional) Sets this ID to be the image ID value, which is used to identify the Cisco IOS device for CNS image agent services. If both optional keywords are omitted, the image ID is set to the host name of the Cisco IOS device.
hardware-serial	Uses the hardware serial number as the unique ID.
hostname	Uses the host name as the unique ID. This is the system default.
string *string*	Uses an arbitrary text string—typically the host name—as the unique ID.

Defaults

The system defaults to the host name of the Cisco IOS device as the unique ID.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced on Cisco IAD2420 series IADs.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.3(1)	The optional **image** keyword was added to set an image ID.

Usage Guidelines

Use this command to set the unique ID to the CNS configuration agent, which then pulls the initial configuration template to the Cisco IOS device during bootup.

You can set one or all three IDs: the config ID value for CNS configuration services, the event ID value for CNS event services, and the image ID value for CNS image agent services. To set all values, use the command three times.

To set the CNS event ID to the host name of the Cisco IOS device, use the **no** form of this command with the **event** keyword. To set the CNS config ID to the host name of the Cisco IOS device, use the **no** form of this command without the **event** keyword. To set the CNS image ID to the host name of the Cisco IOS device, use the **no** form of this command with the **image** keyword.

Examples

The following example shows how to pass the host name of the Cisco IOS device as the config ID value:

```
Router(config)# cns id hostname
```

The following example shows how to pass the hardware serial number of the Cisco IOS device as the event ID value:

```
Router(config)# cns id hardware-serial event
```

The following example shows how to pass the IP address of Ethernet interface 0/1 as the image ID value:

```
Router(config)# cns id ethernet 0/1 image
```

Related Commands

Command	Description
cns event	Enables the CNS event gateway, which provides CNS event services to Cisco IOS clients.
cns image	Enables the CNS image agent services to Cisco IOS clients.

cns image

To configure the CNS image agent services, use the **cns image** command in global configuration mode. To disable the use of CNS image agent services, use the **no** form of this command.

cns image [**server** *server-url* [**status** *status-url*]]

no cns image [**server** *server-url* [**status** *status-url*]]

Syntax Description

server	(Optional) Specifies an image distribution server to contact for information about an updated image to be downloaded.
server-url	(Optional) The URL used to contact an image distribution server. An IP address or domain name can be used.
status	(Optional) Specifies that any status messages generated by CNS image agent operations will be sent to the URL specified by the *status-url* argument.
status-url	(Optional) The URL of a web server to which status messages are written.

Defaults

When configured, the CNS image agent always listens for image events on the CNS Event Bus server.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use the **cns image** command to start the CNS image agent process and to listen for image-related events on the CNS Event Bus.

If the optional server details are specified, the CNS image agent uses the server URL to contact the image management server. If no server details are specified, the URL for the image server must be supplied using one of the following three methods. The first method is to specify the image server using the server options on the **cns image retrieve** command. The second method is to use the server configured by the CNS event agent and stored as an image server event that can be received from the CNS Event Bus. The third method does not require a server URL because it uses CNS Event Bus mode.

If the optional status details are not specified, the status messages are sent as events on the CNS Event Bus.

Examples

The following example shows how to enable the CNS image agent services and configure a path to the image distribution server and a status messages server:

```
Router(config)# cns image server https://10.20.2.3:8080/cns/imageserver/ status
https://10.20.2.3:8080/cns/imageserver/messages/
```

Related Commands

Command	Description
show cns image status	Displays information about the CNS image agent status.

cns image password

To configure a password to use with the CNS image agent services, use the **cns image password** command in global configuration mode. To disable the use of a password, use the **no** form of this command.

cns image password *image-password*

no cns image password *image-password*

Syntax Description

image-password	Password to be used for CNS image agent services.

Defaults

No password is used with the CNS image agent services.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use this command to create a password that is sent along with the image ID in all CNS image agent messages. The receiver of these messages can use this information to authenticate the sending device. This password may be different from the username and password used for HTTP basic authentication configured with other CNS image agent commands.

Examples

The following example shows how to configure a password to be used for the CNS image agent services:

```
Router(config)# cns image password textabc
```

Related Commands

Command	Description
cns id	Specifies the unique event ID, config ID, or image ID used by CNS services.

cns image retrieve

To contact a CNS image distribution server and download a new image if a new image exists, use the **cns image retrieve** command in privileged EXEC mode.

cns image retrieve [**server** *server-url* [**status** *status-url*]]

Syntax Description

server	(Optional) Specifies an image distribution server to contact for information about an updated image to be downloaded. If the **server** keyword is not specified, the server path configured in the **cns image** command is used. If no server path has been configured, an error is displayed.
server-url	(Optional) The URL used to contact an image distribution server. If the *server-url* argument is not specified, the URL path configured in the **cns image** command is used. If no URL has been configured, an error is displayed.
status	(Optional) Specifies that any status messages generated by this command will be sent to the URL specified by the *status-url* argument.
status-url	(Optional) The URL of a web server to which status messages are written.

Defaults

If the **server** keyword and *server-url* argument are not specified, the server path configured in the **cns image** command is used. If no server path has been configured, an error is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

You must enable the CNS image agent services using the **cns image** command before configuring this command.

Use this command to poll an image distribution server and download a new image to the Cisco IOS device if a new image exists.

Examples

The following example shows how to configure the CNS image agent to access the image distribution server at 10.19.2.3 and download a new image if a new image exists:

```
Router# cns image retrieve server https://10.20.2.3:8080/cns/imageserver/ status
https://10.20.2.3:8080/cns/imageserver/messages/
```

Related Commands

Command	Description
cns image	Enables CNS image agent services.
cns trusted-server	Specifies a trusted server for CNS agents.
show cns image status	Displays information about the CNS image agent status.

cns image retry

To set the CNS image upgrade retry interval, use the **cns image retry** command in global configuration mode. To restore the default value, use the **no** form of this command.

cns image retry *seconds*

no cns image retry *seconds*

Syntax Description

seconds	(Optional) Interval in seconds from 0 to 65535. The default is 60 seconds.

Defaults

Retry interval is 60 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use this command to set an interval after which the CNS image agent will retry an image upgrade operation if the original upgrade attempt failed.

Examples

The following example shows how to set the CNS image upgrade interval to 240 seconds:

```
Router(config)# cns image retry 240
```

Related Commands

Command	Description
cns image	Enables CNS image agent services.

cns inventory

To enable the CNS inventory agent—that is, to send an inventory of the router's line cards and modules to the CNS configuration engine—and enter CNS inventory mode, use the **cns inventory** command in global configuration mode. To disable the CNS inventory agent, use the **no** form of this command.

cns inventory

no cns inventory

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.3(1)	The **config**, **event**, and **notify oir** keywords were removed.

Usage Guidelines

Use this command with the **announce config** and **transport event** CNS inventory configuration mode commands to specify when to notify the CNS configuration engine of changes to the router's port-adaptor and interface inventory. A transport must be specified in CNS inventory configuration mode before any of the CNS inventory commands are executed.

Examples

The following example shows how to enable the CNS inventory agent and enter CNS inventory configuration mode:

```
Router(config)# cns inventory
Router(cns_inv)#
```

Related Commands

Command	Description
announce config	Species that an unsolicited configuration inventory is sent out by the CNS inventory agent at bootup.
cns config initial	Starts the CNS configuration agent and initiates an initial configuration.
transport events	Species that inventory events are sent out by the CNS inventory agent.

cns mib-access encapsulation

To specify whether Cisco Networking Services (CNS) should use nongranular (SNMP) or granular (XML) encapsulation to access MIBs, use the **cns mib-access encapsulation** command in global configuration mode. To disable the currently specified encapsulation, use the **no** form of this command.

cns mib-access encapsulation {**snmp** | **xml** [**size** *bytes*]}

no cns mib-access encapsulation {**snmp** | **xml**}

Syntax Description

snmp	Enables nongranular (SNMP) encapsulation for MIB access.
xml	Enables granular (XML) encapsulation for MIB access.
size *bytes*	(Optional) Maximum size in bytes for response events. The default is 3072.

Defaults

For XML encapsulation, a maximum size of 3072 bytes.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced on Cisco 2600 series and Cisco 3600 series routers.

Examples

The following example specifies that XML be used to access MIBs:

```
Router(config)# cns mib-access encapsulation xml
```

Related Commands

Command	Description
cns notifications encapsulation	Specifies whether CNS notifications should be sent using nongranular (SNMP) or granular (XML) encapsulation.

cns notifications encapsulation

To specify whether Cisco Networking Services (CNS) notifications should be sent using nongranular (SNMP) or granular (XML) encapsulation, use the **cns notifications encapsulation** command in global configuration mode. To disable the currently specified encapsulation, use the **no** form of this command.

cns notifications encapsulation {**snmp** | **xml**}

no cns notifications encapsulation {**snmp** | **xml**}

Syntax Description

snmp	Uses nongranular (SNMP) encapsulation to send notifications.
xml	Uses granular (XML) encapsulation to send notifications.

Defaults

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced on Cisco 2600 series and Cisco 3600 series routers.

Examples

The following example shows how to specify that granular notifications should be sent:

```
Router(config)# cns notifications encapsulation xml
```

Related Commands

Command	Description
cns mib-access encapsulation	Specifies whether CNS should use granular (XML) or nongranular (SNMP) encapsulation to access MIBs.

cns template connect

To enter Cisco Networking Services (CNS) template connect configuration mode and define the name of a CNS connect template, use the **cns template connect** command in global configuration mode. To disable the CNS connect template, use the **no** form of this command.

cns template connect *name*

no cns template connect *name*

Syntax Description

name	The name of the CNS connect template to be configured.

Defaults

No CNS connect templates are defined.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.3(9)	This command was integrated into Cisco IOS Release 12.3(9).

Usage Guidelines

Use the **cns template connect** command to enter CNS template connect configuration mode and define the name of the CNS connect template to be configured. Then use the **cli** command to specify the command lines of the CNS connect template.

Note When creating a CNS connect template, you must enter the **exit** command to complete the configuration of the template and exit from CNS template connect configuration mode. This requirement was implemented to prevent accidentally entering a command without the **cli** command.

Note Effective with Cisco IOS Releases 12.3(8)T and 12.3(9), the **cns config connect-intf** command is replaced by the **cns connect** and **cns template connect** commands.

Examples

The following example shows how to configure a CNS connect template named template1:

```
Router (config)# cns template connect template-1
Router (config-templ-conn)# cli command-1
Router (config-templ-conn)# cli command-2
Router (config-templ-conn)# cli no command-3
Router (config-templ-conn)# exit
Router (config)#
```

When the template1 template is applied, the following commands are sent to the router's parser:

```
command-1
command-2
no command-3
```

When the template1 template is removed from the router's configuration after an unsuccessful ping attempt to the CNS configuration engine, the following commands are sent to the router's parser:

```
no command-1
no command-2
command-3
```

Related Commands

Command	Description
cli (cns)	Specifies the command lines of a CNS connect template.
cns connect	Enters CNS connect configuration mode and defines the parameters of a CNS connect profile for connecting to the CNS configuration engine.
discover (cns)	Defines the interface parameters within a CNS connect profile for connecting to the CNS configuration engine.
template (cns)	Specifies a list of CNS connect templates within a CNS connect profile to be applied to a router's configuration.

cns trusted-server

To specify a trusted server for CNS agents, use the **cns trusted-server** command in global configuration mode. To disable the use of a trusted server for a CNS agent, use the **no** form of this command.

cns trusted-server {**all-agents** | **config** | **event** | **exec** | **image**} *hostname* | *ip-address*

no cns trusted-server {**all-agents** | **config** | **event** | **exec** | **image**}

Syntax Description

all-agents	Specifies a trusted server for all CNS agents.
config	Specifies a trusted server for CNS config agent.
event	Specifies a trusted server for CNS event agent.
exec	Specifies a trusted server for CNS exec agent.
image	Specifies a trusted server for CNS image agent.
hostname	Host name of the trusted server.
ip-address	IP address of the trusted server.

Defaults

all-agents

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use the **cns trusted-server** command to specify a trusted server for an individual CNS agent or all the CNS agents. In previous Cisco IOS Releases CNS agents could connect to any server and this could expose the system to security violations. An attempt to connect to a server not on the list will result in an error message being displayed. For backwards compatibility the configuration of a server address using the configuration command-line interface (CLI) for a CNS agent will result in an implicit trust of the server. The implicit trusted server commands apply only to commands in configuration mode, not EXEC mode commands.

Use this command when a CNS agent will redirect its response to a server address that is not explicitly configured on the command line for the specific CNS agent. For example, the CNS exec agent may have one server configured but receive a message from the CNS Event Bus that overrides the configured server. The new server address has not been explicitly configured so the new server address is not a trusted server. An error will be generated when the CNS exec agent tries to respond to this new server address unless the **cns trusted-server** command has been configured for the new server address.

Examples

The following example shows how to configure server 10.19.2.5 as a trusted server for the CNS event agent:

```
Router# cns trusted-server event 10.19.2.5
```

The following example shows how to configure server 10.2.2.8 as an implicit trusted server for the CNS image agent:

```
Router# cns image server 10.2.2.8 status 10.2.2.8
```

Related Commands

Command	Description
cns config	Configures CNS configuration agent services.
cns event	Enables and configures CNS event agent services.
cns image	Configures CNS image agent services.

config-cli

Note Effective with Cisco IOS Releases 12.3(8)T and 12.3(9), the **config-cli** command is replaced by the **cli (cns)** command. See the **cli (cns)** command for more information.

To connect to the Cisco Networking Services (CNS) configuration engine using a specific type of interface, use the **config-cli** command in CNS Connect-interface configuration mode.

config-cli *type* [*number*]

Syntax Description

type number	Type of interface. Indicates from which interface the IP or MAC address should be retrieved in order to define the unique ID.
number	(Optional) Interface number. Indicates from which interface the IP or MAC address should be retrieved in order to define the unique ID.

Defaults

No command lines are specified to configure the interface.

Command Modes

CNS Connect-interface configuration

Command History

Release	Modification
12.2(8)T	This command was introduced on Cisco 2600 series and Cisco 3600 series routers.
12.3(8)T	This command was replaced by the **cli (cns)** command.
12.3(9)	This command was replaced by the **cli (cns)** command.

Usage Guidelines

Begin by using the **cns config connect-intf** command to enter CNS Connect-interface configuration (config-cns-conn-if) mode. Then use either this or its companion CNS bootstrap-configuration command to connect to the CNS configuration engine for initial configuration:

- **config-cli** connects to the registrar using a specific type of interface. You must specify the interface type but need not specify the interface number; the router's bootstrap configuration finds the connecting interface, regardless of the slot in which the card resides, by trying different candidate interfaces until it can ping the configuration engine.
- **line-cli** connects to the registrar using modem dialup lines.

Immediately after either of the commands, enter additional configuration commands as appropriate.

Examples

The following example enters CNS Connect-interface configuration mode, connects to a configuration engine using an asynchronous interface, and issues a number of commands:

```
Router(config)# cns config connect-intf Async
Router(config-cns-conn-if)# config-cli encapsulation ppp
```

```
Router(config-cns-conn-if)# config-cli ip unnumbered FastEthernet0/0
Router(config-cns-conn-if)# config-cli dialer rotary-group 0
Router(config-cns-conn-if)# line-cli modem InOut
Router(config-cns-conn-if)# line-cli
.
.
.
Router(config-cns-conn-if)# exit
```

These commands apply the following configuration:

```
line 65
modem InOut
.
.
.
interface Async65
encapsulation ppp
dialer in-band
dialer rotary-group 0
```

Related Commands

Command	Description
cns config connect-intf	Specifies the interface for connecting to the CNS configuration engine.
line-cli	Connects to the CNS configuration engine using a modem dialup line.

config-register

To change the configuration register settings, use the **config-register** command in global configuration mode.

config-register *value*

Syntax Description

value	Hexadecimal or decimal value that represents the 16-bit configuration register value that you want to use the next time the router is restarted. The value range is from 0x0 to 0xFFFF (0 to 65535 in decimal).

Defaults

Refer to the documentation for your platform for the default configuration register value. For many newer platforms, the default is 0x2102, which causes the router to boot from Flash memory and the Break key to be ignored.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command applies only to platforms that use a software configuration register.

The lowest four bits of the configuration register (bits 3, 2, 1, and 0) form the boot field. The boot field determines if the router boots manually, from ROM, or from Flash or the network.

To change the boot field value and leave all other bits set to their default values, follow these guidelines:

- If you set the configuration register boot field value to 0x0, you must boot the operating system manually with the **boot** command.
- If you set the configuration register boot field value to 0x1, the router boots using the default ROM software.
- If you set the configuration register boot field to any value from 0x2 to 0xF, the router uses the boot field value to form a default boot filename for booting from a network server.

For more information about the configuration register bit settings and default filenames, refer to the appropriate router hardware installation guide.

Examples

In the following example, the configuration register is set to boot the system image from Flash memory:

```
config-register 0x2102
```

Related Commands

Command	Description
boot system	Specifies the system image that the router loads at startup.
confreg	Changes the configuration register settings while in ROM monitor mode.
o	Lists the value of the boot field (bits 0 to 3) in the configuration register.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

configure memory

To configure the system from the system memory, use the **configure memory** command in privileged EXEC mode.

configure memory

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

On all platforms except Class A Flash file system platforms, this command executes the commands located in the configuration file in NVRAM (the "startup configuration file").

On Class A Flash file system platforms, if you specify the **configure memory** command, the router executes the commands pointed to by the CONFIG_FILE environment variable. The CONFIG_FILE environment variable specifies the location of the configuration file that the router uses to configure itself during initialization. The file can be located in NVRAM or any of the Flash file systems supported by the platform.

When the CONFIG_FILE environment variable specifies NVRAM, the router executes the NVRAM configuration only if it is an entire configuration, not a distilled version. A distilled configuration is one that does not contain access lists.

To view the contents of the CONFIG_FILE environment variable, use the **show bootvar** EXEC command. To modify the CONFIG_FILE environment variable, use the **boot config** command and then save your changes by issuing the **copy system:running-config nvram:startup-config** command.

Examples

In the following example, a router is configured from the configuration file in the memory location pointed to by the CONFIG_FILE environment variable:

```
Router# configure memory
```

Related Commands

Command	Description
boot config	Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).
copy system:running-config nvram:startup-config	Saves the running configuration as the startup configuration file.
show bootvar	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.

configure network

The **configure network** command was replaced by the **copy** {**rcp** | **tftp**} **running-config** command in Cisco IOS Release 11.0. To maintain backward compatibility, the **configure network** command continues to function in Cisco IOS Release 12.2(11)T for most systems, but support for this command may be removed in a future release.

The **copy** {**rcp** | **tftp**} **running-config** command was replaced by the **copy** {**ftp:** | **rcp:** | **tftp:**}[*filename*] **system:running-config** command in Cisco IOS Release 12.1.

The **copy** {**ftp:** | **rcp:** | **tftp:**}[*filename*] **system:running-config** command specifies that a configuration file should be copied from a FTP, rcp, or TFTP source to the running configuration. See the description of the **copy** command in this chapter for more information.

configure overwrite-network

The **configure overwrite-network** has been replaced by the **copy** {*ftp-url* | *rcp-url* | *tftp-url*} **nvram:startup-config** command. See the description of the **copy** command in the **"Cisco IOS File System Commands"** chapter for more information.

configure terminal

To enter global configuration mode, use the **configure terminal** command in privileged EXEC mode.

configure terminal

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command to enter global configuration mode. Note that commands in this mode are written to the running configuration file as soon as you enter them (using the Enter key/Carriage Return).

After you enter the **configure** command, the system prompt changes from `<router-name>#` to `<router-name>(config)#`, indicating that the router is in global configuration mode. To leave global configuration mode and return to privileged EXEC mode, type **end** or press **Ctrl-Z**.

To view the changes to the configuration you have made, use the **more system:running-config** command or **show running-config** command in EXEC mode.

Examples

In the following example, the user enters global configuration mode:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Related Commands

Command	Description
boot config	Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).
copy running-config startup-config OR **copy system:running-config nvram:startup-config**	Saves the running configuration as the startup configuration file.
show running-config OR **more system:running-config**	Displays the currently running configuration.

confreg

To change the configuration register settings while in ROM monitor mode, use the **confreg** command in ROM monitor mode.

confreg [*value*]

Syntax Description

value	(Optional) Hexadecimal value that represents the 16-bit configuration register value that you want to use the next time the router is restarted. The value range is from 0x0 to 0xFFFF.

Defaults

Refer to your platform documentation for the default configuration register value.

Command Modes

ROM monitor

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Not all versions in the ROM monitor support this command. Refer to your platform documentation for more information on ROM monitor mode.

If you use this command without specifying the configuration register value, the router prompts for each bit of the configuration register.

The lowest four bits of the configuration register (bits 3, 2, 1, and 0) form the boot field. The boot field determines if the router boots manually, from ROM, or from Flash or the network.

To change the boot field value and leave all other bits set to their default values, follow these guidelines:

- If you set the configuration register boot field value to 0x0, you must boot the operating system manually with the **boot** command.
- If you set the configuration register boot field value to 0x1, the router boots using the default ROM software.
- If you set the configuration register boot field to any value from 0x2 to 0xF, the router uses the boot field value to form a default boot filename for booting from a network server.

For more information about the configuration register bit settings and default filenames, refer to the appropriate router hardware installation guide.

Examples

In the following example, the configuration register is set to boot the system image from Flash memory:

```
confreg 0x210F
```

In the following example, no configuration value is entered, so the system prompts for each bit in the register:

```
rommon 7 > confreg

     Configuration Summary
enabled are:
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:  y
enable  "diagnostic mode"? y/n  [n]:  y
enable  "use net in IP bcast address"? y/n  [n]:

enable  "load rom after netboot fails"? y/n  [n]:
enable  "use all zero broadcast"? y/n  [n]:
enable  "break/abort has effect"? y/n  [n]:
enable  "ignore system config info"? y/n  [n]:
change console baud rate? y/n  [n]:  y
enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400  [0]:  0
change the boot characteristics? y/n  [n]:  y
enter to boot:
 0 = ROM Monitor
 1 = the boot helper image
 2-15 = boot system
    [0]:  0

     Configuration Summary
enabled are:
diagnostic mode
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:

You must reset or power cycle for new config to take effect.
rommon 8>
```

continue

To return to EXEC mode from ROM monitor mode, use the **continue** command in ROM monitor mode.

continue

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

ROM monitor

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Use this command to return to EXEC mode from ROM monitor mode, to use the system image instead of reloading. On older platforms, the angle bracket (< >) indicates that the router is in ROM monitor mode. On newer platforms, `rommon number>` is the default ROM monitor prompt. Typically, the router is in ROM monitor mode when you manually load a system image or perform diagnostic tests. Otherwise, the router will most likely never be in this mode.

Caution While in ROM monitor mode, the Cisco IOS system software is suspended until you issue either a reset or the **continue** command.

Examples

In the following example, the **continue** command switches the router from ROM monitor to EXEC mode:

```
> continue
Router#
```

Related Commands

Command	Description
boot	Boots the router manually.

copy

To copy any file from a source to a destination, use the **copy** command in EXEC mode.

copy [**/erase**] *source-url destination-url*

Syntax Description

/erase	(Optional) Erases the destination file system before copying.
source-url	The location URL or alias of the source file or directory to be copied.
destination-url	The destination URL or alias of the copied file or directory.

The exact format of the source and destination URLs varies according to the file or directory location. You may enter either an alias keyword for a particular file or an alias keyword for a file system type (not a file within a type).

Timesaver Aliases are used to cut down on the amount of typing you need to perform. For example, it is easier to type **copy run start** (the abbreviated form of the **copy running-config startup-config** command) than it is to type **copy system:r nvram:s** (the abbreviated form of the **copy system:running-config nvram:startup-config** command). These aliases also allow you to continue using some of the common commands used in previous versions of Cisco IOS software.

Table 15 shows two keyword shortcuts to URLs.

Table 15 Common Keyword Aliases to URLs

Keyword	Source or Destination
running-config	(Optional) Keyword alias for the **system:running-config** URL. The **system:running-config** keyword represents the current running configuration file. This keyword does not work in **more** and **show file** EXEC command syntaxes.
startup-config	(Optional) Keyword alias for the **nvram:startup-config URL.** The **nvram:startup-config** keyword represents the configuration file used during initialization (startup). This file is contained in NVRAM for all platforms except the Cisco 7000 family, which uses the CONFIG_FILE environment variable to specify the startup configuration. The Cisco 4500 series cannot use the **copy running-config startup-config** command. This keyword does not work in **more** and **show file** EXEC command syntaxes.

The following tables list aliases by file system type. If you do not specify an alias, the router looks for a file in the current directory.

Table 16 lists URL aliases for Special (opaque) file systems. Table 17 lists them for network file systems, and Table 18 lists them for local writable storage.

Table 16 URL Prefix Aliases for Special File Systems

Alias	Source or Destination
flh:	Source URL for flash load helper log files.
modem:	Destination URL for loading modem firmware on Cisco 5200 and 5300 Series routers.
nvram:	Router NVRAM. You can copy the startup configuration into or from NVRAM. You can also display the size of a private configuration file.
null:	Null destination for copies or files. You can copy a remote file to null to determine its size.
system:	Source or destination URL for system memory, which includes the running configuration.
xmodem:	Source destination for the file from a network machine that uses the Xmodem protocol.
ymodem:	Source destination for the file from a network machine that uses the Xmodem protocol.

Table 17 URL Prefix Aliases for Network File Systems

Alias	Source or Destination
ftp:	Source or destination URL for an File Transfer Protocol (FTP) network server. The syntax for this alias is as follows: **ftp:**[[[*//username* [*:password*]*@*]*location*]*/directory*]*/filename.*
rcp:	Source or destination URL for a Remote Copy Protocol (rcp) network server. The syntax for this alias is as follows: **rcp:**[[[*//username@*]*location*]*/directory*]*/filename.*
tftp:	Source or destination URL for a TFTP network server. The syntax for this alias is **tftp:**[[*//location*]*/directory*]*/filename.*

Table 18 URL Prefix Aliases for Local Writable Storage File Systems

Alias	Source or Destination
bootflash:	Source or destination URL for boot flash memory.
disk0: and disk1:	Source or destination URL of rotating media.
flash:	Source or destination URL for Flash memory. This alias is available on all platforms. For platforms that lack a flash: device, note that **flash:** is aliased to **slot0:**, allowing you to refer to the main Flash memory storage area on all platforms.
slavebootflash:	Source or destination URL for internal Flash memory on the slave RSP card of a router configured for HSA.
slaveram:	NVRAM on a slave RSP card of a router configured for HSA.
slaveslot0:	Source or destination URL of the first PCMCIA card on a slave RSP card of a router configured for HSA.

Table 18 URL Prefix Aliases for Local Writable Storage File Systems (continued)

Alias	Source or Destination
slaveslot1:	Source or destination URL of the second PCMCIA slot on a slave RSP card of a router configured for HSA.
slot0:	Source or destination URL of the first PCMCIA Flash memory card.
slot1:	Source or destination URL of the second PCMCIA Flash memory card.

Command Modes

EXEC

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

You can enter on the command line all necessary source- and destination-URL information and the username and password to use, or you can enter the **copy** command and have the router prompt you for any missing information.

If you enter information, choose one of the following three options: **running-config**, **startup-config**, or a file system alias (see previous tables). The location of a file system dictates the format of the source or destination URL.

The colon is required after the alias. However, earlier commands not requiring a colon remain supported, but are unavailable in context-sensitive help.

The entire copying process may take several minutes and differs from protocol to protocol and from network to network.

In the alias syntax for **ftp:**, **rcp:**, and **tftp:**, the location is either an IP address or a host name. The filename is specified relative to the directory used for file transfers.

This section contains usage guidelines for the following topics:

- Understanding Invalid Combinations of Source and Destination
- Understanding Character Descriptions
- Understanding Partitions
- Using rcp
- Using FTP
- Storing Images on Servers
- Copying from a Server to Flash Memory
- Verifying Images
- Copying a Configuration File from a Server to the Running Configuration
- Copying a Configuration File from a Server to the Startup Configuration
- Storing the Running or Startup Configuration on a Server
- Saving the Running Configuration to the Startup Configuration

- Using CONFIG_FILE, BOOT, and BOOTLDR Environment Variables
- Using the Copy Command with the Dual RSP Feature

Understanding Invalid Combinations of Source and Destination

Some invalid combinations of source and destination exist. Specifically, you cannot copy the following:

- From a running configuration to a running configuration
- From a startup configuration to a startup configuration
- From a device to the same device (for example, the **copy flash: flash:** command is invalid)

Understanding Character Descriptions

Table 19 describes the characters that you may see during processing of the **copy** command.

Table 19 copy Character Descriptions

Character	Description
!	For network transfers, an exclamation point indicates that the copy process is taking place. Each exclamation point indicates the successful transfer of ten packets (512 bytes each).
.	For network transfers, a period indicates that the copy process timed out. Many periods in a row typically mean that the copy process may fail.
O	For network transfers, an uppercase O indicates that a packet was received out of order and the copy process may fail.
e	For Flash erasures, a lowercase e indicates that a device is being erased.
E	An uppercase E indicates an error. The copy process may fail.
V	A series of uppercase Vs indicates the progress during the verification of the image checksum.

Understanding Partitions

You cannot copy an image or configuration file to a Flash partition from which you are currently running. For example, if partition 1 is running the current system image, copy the configuration file or image to partition 2. Otherwise, the copy operation will fail.

You can identify the available Flash partitions by entering the **show file system** EXEC command.

Using rcp

The rcp requires a client to send a remote username upon each rcp request to a server. When you copy a configuration file or image between the router and a server using rcp, the Cisco IOS software sends the first valid username it encounters in the following sequence:

1. The remote username specified in the **copy** command, if a username is specified.
2. The username set by the **ip rcmd remote-username** global configuration command, if the command is configured.
3. The remote username associated with the current tty (terminal) process. For example, if the user is connected to the router through Telnet and was authenticated through the **username** command, the router software sends the Telnet username as the remote username.
4. The router host name.

For the rcp copy request to process, an account must be defined on the network server for the remote username. If the network administrator of the destination server did not establish an account for the remote username, this command will not run. If the server has a directory structure, the configuration file or image is written to or copied from the directory associated with the remote username on the server. For example, if the system image resides in the home directory of a user on the server, specify that user name as the remote username.

If you are writing to the server, the rcp server must be properly configured to accept the rcp write request from the user on the router. For UNIX systems, add an entry to the *.rhosts* file for the remote user on the rcp server. Suppose the router contains the following configuration lines:

```
hostname Rtr1
ip rcmd remote-username User0
```

If the router IP address translates to Router1.company.com, then the *.rhosts* file for User0 on the rcp server should contain the following line:

```
Router1.company.com Rtr1
```

Refer to the documentation for your rcp server for more details.

If you are using a personal computer as a file server, the computer must support the remote shell protocol (rsh).

Using FTP

The FTP protocol requires a client to send a username and password with each FTP request to a remotre FTP server. Use the **ip ftp username** and **ip ftp password** global configuration commands to specify a default username and password for all copy operations to or from an FTP server. Include the username in the **copy** command syntax if you want to specify a username for that copy operation only.

When you copy a configuration file from the router to a server using FTP, the Cisco IOS software sends the first valid username that it encounters in the following sequence:

1. The username specified in the **copy** command, if a username is specified.
2. The username set by the **ip ftp username** command, if the command is configured.
3. Anonymous.

The router sends the first valid password in the following list:

1. The password specified in the **copy** command, if a password is specified.
2. The password set by the **ip ftp password** command, if the command is configured.
3. The router forms a password *username@routername.domain*. The variable *username* is the username associated with the current session, *routername* is the configured host name, and *domain* is the domain of the router.

The username and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept the FTP write request from the user on the router.

If the server has a directory structure, the configuration file or image is written to or copied from the directory associated with the username on the server. For example, if the system image resides in the home directory of a user on the server, specify that user name as the remote username.

Refer to the documentation for your FTP server for more details.

Storing Images on Servers

Use the **copy flash:** *destination-url* command (for example, **copy flash: tftp:**) to copy a system image or boot image from Flash memory to a network server. You can use the copy of the image as a backup copy. Also, you can also use the image backup file to verify that the image in Flash memory is the same as that in the original file.

Copying from a Server to Flash Memory

Use the **copy** *destination-url* **flash:** command (for example, **copy tftp: flash:**) to copy an image from a server to Flash memory.

On Class B file system platforms, the system provides an option to erase existing Flash memory before writing onto it.

Note Verify the image in Flash memory before booting the image.

Verifying Images

When copying a new image to your router, you should confirm that the image was not corrupted during the copy process. Depending on the destination filesystem type, a checksum for the image file may be displayed when the **copy** command completes. You can verify this checksum by comparing it to the checksum value provided for your image file on Cisco.com.

Caution If the checksum values do not match, do not reboot the router. Instead, reissue the **copy** command and compare the checksums again. If the checksum is repeatedly wrong, copy the original image back into Flash memory *before* you reboot the router from Flash memory. If you have a corrupted image in Flash memory and try to boot from Flash memory, the router will start the system image contained in ROM (assuming booting from a network server is not configured). If ROM does not contain a fully functional system image, the router might not function and will need to be reconfigured through a direct console port connection.

An alternate method for file verification is to use the UNIX 'diff' command. This method can also be applied to file types other than Cisco IOS images. If you suspect that a file is corrupted, copy the suspect file and the original file to a Unix server. (The file names may need to be modified if you try to save the files in the same directory.) Then run the UNIX 'diff' command on the two files. If there is no difference, then the file has not been corrupted.

Copying a Configuration File from a Server to the Running Configuration

Use the **copy** {**ftp:** | **rcp:** | **tftp:**} **running-config** command to load a configuration file from a network server to the running configuration of the router (note that **running-config** is the alias for the **system:running-config** keyword). The configuration will be added to the running configuration as if the commands were typed in the command-line interface (CLI). Thus, the resulting configuration file will be a combination of the previous running configuration and the loaded configuration file, with the loaded configuration file having precedence.

You can copy either a host configuration file or a network configuration file. Accept the default value of *host* to copy and load a host configuration file containing commands that apply to one network server in particular. Enter *network* to copy and load a network configuration file containing commands that apply to all network servers on a network.

Copying a Configuration File from a Server to the Startup Configuration

Use the **copy** {**ftp:** | **rcp:** | **tftp:**} **nvram:startup-config** command to copy a configuration file from a network server to the router startup configuration. These commands replace the startup configuration file with the copied configuration file.

Storing the Running or Startup Configuration on a Server

Use the **copy system:running-config** {**ftp:** | **rcp:** | **tftp:**} command to copy the current configuration file to a network server using FTP, rcp, or TFTP. Use the **copy nvram:startup-config** {**ftp:** | **rcp:** | **tftp:**} command to copy the startup configuration file to a network server.

The configuration file copy can serve as a backup copy.

Saving the Running Configuration to the Startup Configuration

Use the **copy system:running-config nvram:startup-config** command to copy the running configuration to the startup configuration.

Note Some specific commands might not get saved to NVRAM. You will need to enter these commands again if you reboot the machine. These commands are noted in the documentation. We recommend that you keep a listing of these settings so you can quickly reconfigure your router after rebooting.

If you issue the **copy system:running-config nvram:startup-config** command from a bootstrap system image, a warning will instruct you to indicate whether you want your previous NVRAM configuration to be overwritten and configuration commands to be lost. This warning does not appear if NVRAM contains an invalid configuration or if the previous configuration in NVRAM was generated by a bootstrap system image.

On all platforms except Class A file system platforms, the **copy system:running-config nvram:startup-config** command copies the currently running configuration to NVRAM.

On the Class A Flash file system platforms, the **copy system:running-config nvram:startup-config** command copies the currently running configuration to the location specified by the CONFIG_FILE environment variable. This variable specifies the device and configuration file used for initialization. When the CONFIG_FILE environment variable points to NVRAM or when this variable does not exist (such as at first-time startup), the software writes the current configuration to NVRAM. If the current configuration is too large for NVRAM, the software displays a message and stops executing the command.

When the CONFIG_FILE environment variable specifies a valid device other than **nvram:** (that is, **flash:**, **bootflash:**, **slot0:**, or **slot1:**), the software writes the current configuration to the specified device and filename, and stores a distilled version of the configuration in NVRAM. A distilled version is one that does not contain access list information. If NVRAM already contains a copy of a complete configuration, the router prompts you to confirm the copy.

Using CONFIG_FILE, BOOT, and BOOTLDR Environment Variables

For the Class A Flash file system platforms, specifications are as follows:

- The CONFIG_FILE environment variable specifies the configuration file used during router initialization.
- The BOOT environment variable specifies a list of bootable images on various devices.
- The BOOT environment variable specifies a list of bootable images on various devices.
- The BOOTLDR environment variable specifies the Flash device and filename containing the rxboot image that ROM uses for booting.

- Cisco 3600 routers do not use a dedicated boot helper image (rxboot), which many other routers use to help with the boot process. Instead, the BOOTLDR ROM monitor environment variable identifies the Flash memory device and filename that are used as the boot helper; the default is the first system image in Flash memory.

To view the contents of environment variables, use the **show bootvar** EXEC command. To modify the CONFIG_FILE environment variable, use the **boot config** global configuration command. To modify the BOOTLDR environment variable, use the **boot bootldr** global configuration command. To modify the BOOT environment variable, use the **boot system** global configuration command. To save your modifications, use the **copy system:running-config nvram:startup-config** command.

When the destination of a **copy** command is specified by the CONFIG_FILE or BOOTLDR environment variable, the router prompts you for confirmation before proceeding with the copy. When the destination is the only valid image in the BOOT environment variable, the router also prompts you for confirmation before proceeding with the copy.

Using the Copy Command with the Dual RSP Feature

The Dual RSP feature allows you to install two Route Switch Processor (RSP) cards in a single router on the Cisco 7507 and Cisco 7513 platforms.

On a Cisco 7507 or Cisco 7513 router configured for Dual RSPs, if you copy a file to **nvram:startup-configuration** with automatic synchronization disabled, the system asks if you also want to copy the file to the slave startup configuration. The default answer is **yes**. If automatic synchronization is enabled, the system automatically copies the file to the slave startup configuration each time you use a **copy** command with **nvram:startup-configuration** as the destination.

Examples

The following examples illustrate uses of the **copy** command.

- Copying an Image from a Server to Flash Memory Examples
- Saving a Copy of an Image on a Server Examples
- Copying a Configuration File from a Server to the Running Configuration Example
- Copying a Configuration File from a Server to the Startup Configuration Example
- Copying the Running Configuration to a Server Example
- Copying the Startup Configuration to a Server Example
- Saving the Current Running Configuration Example
- Moving Configuration Files to Other Locations Examples
- Copying an Image from the Master RSP Card to the Slave RSP Card Example

Copying an Image from a Server to Flash Memory Examples

The following three examples use a **copy rcp:**, **copy tftp:**, or **copy ftp:** command to copy an image file from a server to Flash memory:

- Copying an Image from a Server to Flash Memory Example
- Copying an Image from a Server to a Flash Memory Using Flash Load Helper Example
- Copying an Image from a Server to a Flash Memory Card Partition Example

Copying an Image from a Server to Flash Memory Example

This example copies a system image named file1 from the remote rcp server with an IP address of 172.16.101.101 to Flash memory. On Class B file system platforms, the Cisco IOS software allows you to first erase the contents of Flash memory to ensure that enough Flash memory is available to accommodate the system image.

```
Router# copy rcp://netadmin@172.16.101.101/file1 flash:file1

Destination file name [file1]?
Accessing file 'file1' on 172.16.101.101...
Loading file1 from 172.16.101.101 (via Ethernet0): ! [OK]

Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]

Copy 'file1' from server
  as 'file1' into Flash WITH erase? [yes/no] yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee...erased
Loading file1 from 172.16.101.101 (via Ethernet0): !
[OK - 984/8388608 bytes]

Verifying checksum... OK (0x14B3)
Flash copy took 0:00:01 [hh:mm:ss]
```

Copying an Image from a Server to a Flash Memory Using Flash Load Helper Example

The following example copies a system image into a partition of Flash memory. The system will prompt for a partition number only if there are two or more read/write partitions or one read-only and one read/write partition and dual Flash bank support in boot ROMs. If the partition entered is not valid, the process terminates. You can enter a partition number, a question mark (**?**) for a directory display of all partitions, or a question mark and a number (**?***number*) for directory display of a particular partition. The default is the first read/write partition. In this case, the partition is read-only and has dual Flash bank support in boot ROM, so the system uses Flash Load Helper.

```
Router# copy tftp: flash:

System flash partition information:
Partition   Size     Used    Free    Bank-Size   State       Copy-Mode
    1       4096K    2048K   2048K   2048K       Read Only   RXBOOT-FLH
    2       4096K    2048K   2048K   2048K       Read/Write  Direct

[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 2]

                                **** NOTICE ****
Flash load helper v1.0
This process will accept the copy options and then terminate
the current system image to use the ROM based image for the copy.
Routing functionality will not be available during that time.
If you are logged in via telnet, this connection will terminate.
Users with console access can see the results of the copy operation.
                                ---- ******** ----
Proceed? [confirm]
System flash directory, partition 1:
File  Length   Name/status
  1   3459720  master/igs-bfpx.100-4.3
[3459784 bytes used, 734520 available, 4194304 total]
Address or name of remote host [255.255.255.255]? 172.16.1.1
Source file name? master/igs-bfpx-100.4.3
Destination file name [default = source name]?

Loading master/igs-bfpx.100-4.3 from 172.16.1.111: !
```

```
Erase flash device before writing? [confirm]
Flash contains files. Are you sure? [confirm]
Copy 'master/igs-bfpx.100-4.3' from TFTP server
as 'master/igs-bfpx.100-4.3' into Flash WITH erase? [yes/no] yes
```

Copying an Image from a Server to a Flash Memory Card Partition Example

The following example copies the file c3600-i-mz from the rcp server at IP address 172.23.1.129 to the Flash memory card in slot 0 of a Cisco 3600 series router, which has only one partition. As the operation progresses, the Cisco IOS software asks you to erase the files on the Flash memory PC card to accommodate the incoming file. This entire operation takes 18 seconds to perform, as indicated at the end of the example.

```
Router# copy rcp: slot0:

PCMCIA Slot0 flash

Partition   Size    Used      Free      Bank-Size  State          Copy Mode
  1         4096K   3068K     1027K     4096K      Read/Write     Direct
  2         4096K   1671K     2424K     4096K      Read/Write     Direct
  3         4096K      0K     4095K     4096K      Read/Write     Direct
  4         4096K   3825K      270K     4096K      Read/Write     Direct

[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 1]

PCMCIA Slot0 flash directory, partition 1:
File  Length   Name/status
  1   3142288  c3600-j-mz.test
[3142352 bytes used, 1051952 available, 4194304 total]
Address or name of remote host [172.23.1.129]?
Source file name? /tftpboot/images/c3600-i-mz
Destination file name [/tftpboot/images/c3600-i-mz]?
Accessing file '/tftpboot/images/c3600-i-mz' on 172.23.1.129...
Connected to 172.23.1.129
Loading 1711088 byte file c3600-i-mz: ! [OK]

Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]

Copy '/tftpboot/images/c3600-i-mz' from server
  as '/tftpboot/images/c3600-i-mz' into Flash WITH erase? [yes/no] yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
Connected to 172.23.1.129
Loading 1711088 byte file c3600-i-mz:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Verifying checksum...  OK (0xF89A)
Flash device copy took 00:00:18 [hh:mm:ss]
```

Saving a Copy of an Image on a Server Examples

The following four examples use **copy** commands to copy image files to a server for storage:

- Copy an Image from Flash Memory to an rcp Server Example
- Copy an Image from a Partition of Flash Memory to a Server Example
- Copying an Image from a Flash Memory File System to an FTP Server Example
- Copying an Image from Boot Flash Memory to a TFTP Server Example

Copy an Image from Flash Memory to an rcp Server Example

The following example copies a system image from Flash Memory to an rcp server using the default remote username. Because the rcp server address and filename are not included in the command, the router prompts for it.

```
Router# copy flash: rcp:

IP address of remote host [255.255.255.255]? 172.16.13.110
Name of file to copy? gsxx
writing gsxx - copy complete
```

Copy an Image from a Partition of Flash Memory to a Server Example

The following example copies an image from a particular partition of Flash memory to an rcp server using a remote username of netadmin1.

The system will prompt if there are two or more partitions. If the partition entered is not valid, the process terminates. You have the option to enter a partition number, a question mark (**?**) for a directory display of all partitions, or a question mark and a number (**?***number*) for a directory display of a particular partition. The default is the first partition.

```
Router# configure terminal
Router# ip rcmd remote-username netadmin1
Router# end
Router# copy flash: rcp:
System flash partition information:
Partition   Size     Used    Free    Bank-Size   State       Copy-Mode
    1       4096K    2048K   2048K   2048K       Read Only   RXBOOT-FLH
    2       4096K    2048K   2048K   2048K       Read/Write  Direct
[Type ?<number> for partition directory; ? for full directory; q to abort]
Which partition? [1] 2

System flash directory, partition 2:
File  Length   Name/status
  1   3459720  master/igs-bfpx.100-4.3
[3459784 bytes used, 734520 available, 4194304 total]
Address or name of remote host [ABC.CISCO.COM]?
Source file name? master/igs-bfpx.100-4.3
Destination file name [master/igs-bfpx.100-4.3]?
Verifying checksum for 'master/igs-bfpx.100-4.3' (file # 1)... OK
Copy 'master/igs-bfpx.100-4.3' from Flash to server
as 'master/igs-bfpx.100-4.3'? [yes/no] yes
!!!!...
Upload to server done
Flash copy took 0:00:00 [hh:mm:ss]
```

Copying an Image from a Flash Memory File System to an FTP Server Example

The following example copies the file c3600-i-mz from partition 1 of the Flash memory card in slot 0 to an FTP server at IP address 172.23.1.129.

```
Router# show slot0: partition 1

PCMCIA Slot0 flash directory, partition 1:
File  Length   Name/status
  1   1711088 c3600-i-mz
[1711152 bytes used, 2483152 available, 4194304 total]

Router# copy slot0:1:c3600-i-mz ftp://myuser:mypass@172.23.1.129/c3600-i-mz
Verifying checksum for '/tftpboot/cisco_rules/c3600-i-mz' (file # 1)...  OK
Copy '/tftpboot/cisco_rules/c3600-i-mz' from Flash to server
```

```
  as 'c3700-i-mz'? [yes/no] yes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Upload to server done
Flash device copy took 00:00:23 [hh:mm:ss]
```

Copying an Image from Boot Flash Memory to a TFTP Server Example

The following example copies an image from boot Flash memory to a TFTP server:

```
Router# copy bootflash:file1 tftp://192.168.117.23/file1

Verifying checksum for 'file1' (file # 1)... OK
Copy 'file1' from Flash to server
  as 'file1'? [yes/no]y
!!!!...
Upload to server done
Flash copy took 0:00:00 [hh:mm:ss]
```

Copying a Configuration File from a Server to the Running Configuration Example

The following example copies and runs a configuration filename host1-confg from the netadmin1 directory on the remote server with an IP address of 172.16.101.101:

```
Router# copy rcp://netadmin1@172.16.101.101/host1-confg system:running-config

Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
Router#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

Copying a Configuration File from a Server to the Startup Configuration Example

The following example copies a configuration file host2-confg from a remote FTP server to the startup configuration. The IP address is172.16.101.101, the remote username is netadmin1, and the remote password is ftppass.

```
Router# copy ftp://netadmin1:ftppass@172.16.101.101/host2-confg nvram:startup-config
Configure using rtr2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file rtr2-confg:![OK]
[OK]
Router#
%SYS-5-CONFIG_NV:Non-volatile store configured from rtr2-config by
FTP from 172.16.101.101
```

Copying the Running Configuration to a Server Example

The following example specifies a remote username of netadmin1. Then it copies the running configuration file named rtr2-confg to the netadmin1 directory on the remote host with an IP address of 172.16.101.101.

```
Router# configure terminal
Router(config)# ip rcmd remote-username netadmin1
Router(config)# end
Router# copy system:running-config rcp:
Remote host[]? 172.16.101.101

Name of configuration file to write [Rtr2-confg]?
Write file rtr2-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
```

Copying the Startup Configuration to a Server Example

The following example copies the startup configuration to a TFTP server:

```
Router# copy nvram:startup-config tftp:

Remote host[]? 172.16.101.101

Name of configuration file to write [rtr2-confg]? <cr>
Write file rtr2-confg on host 172.16.101.101?[confirm] <cr>
![OK]
```

Saving the Current Running Configuration Example

The following example copies the running configuration to the startup configuration. On a Class A Flash file system platform, this command copies the running configuration to the startup configuration specified by the CONFIG_FILE variable.

```
copy system:running-config nvram:startup-config
```

The following example shows the warning that the system provides if you try to save configuration information from bootstrap into the system:

```
Router(boot)# copy system:running-config nvram:startup-config

Warning: Attempting to overwrite an NVRAM configuration written
by a full system image. This bootstrap software does not support
the full configuration command set. If you perform this command now,
some configuration commands may be lost.
Overwrite the previous NVRAM configuration?[confirm]
```

Enter **no** to escape writing the configuration information to memory.

Moving Configuration Files to Other Locations Examples

On some routers, you can store copies of configuration files on a Flash memory device. Five examples follow.

Copying the Startup Configuration to a Flash Memory Device Example

The following example copies the startup configuration file (specified by the CONFIG_FILE environment variable) to a Flash memory card inserted in slot 0:

```
copy nvram:startup-config slot0:router-confg
```

Copying the Running Configuration to a Flash Memory Device Example

The following example copies the running configuration from the router to the Flash memory PC card in slot 0:

```
Router# copy system:running-config slot0:berlin-cfg

Building configuration...

5267 bytes copied in 0.720 secs
```

Copying to the Running Configuration from a Flash Memory Device Example

The following example copies the file named ios-upgrade-1 from the Flash memory card in slot 0 to the running configuration:

```
Router# copy slot0:4:ios-upgrade-1 system:running-config

Copy 'ios-upgrade-1' from flash device
  as 'running-config' ? [yes/no] yes
```

Copying to the Startup Configuration from a Flash Memory Device Example

The following example copies the router-image file from the Flash memory to the startup configuration:

```
copy flash:router-image nvram:startup-config
```

Copying a Configuration File from one Flash Device to Another Example

The following example copies the file running-config from the first partition in internal Flash memory to the Flash memory PC card in slot 1. The checksum of the file is verified, and its copying time of 30 seconds is displayed.

```
Router# copy flash: slot1:

System flash

Partition   Size    Used      Free      Bank-Size  State          Copy Mode
  1         4096K   3070K     1025K     4096K      Read/Write     Direct
  2        16384K   1671K    14712K     8192K      Read/Write     Direct

[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 1]

System flash directory, partition 1:
File  Length   Name/status
  1   3142748  dirt/images/mars-test/c3600-j-mz.latest
  2   850      running-config
[3143728 bytes used, 1050576 available, 4194304 total]

PCMCIA Slot1 flash directory:
File  Length   Name/status
  1   1711088  dirt/images/c3600-i-mz
  2   850      running-config
[1712068 bytes used, 2482236 available, 4194304 total]
Source file name? running-config
Destination file name [running-config]?
Verifying checksum for 'running-config' (file # 2)...  OK
Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]

Copy 'running-config' from flash: device
  as 'running-config' into slot1: device WITH erase? [yes/no] yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
!
 [OK - 850/4194304 bytes]

Flash device copy took 00:00:30 [hh:mm:ss]
Verifying checksum...  OK (0x16)
```

Copying an Image from the Master RSP Card to the Slave RSP Card Example

The following example copies the router-image file from the Flash memory card inserted in slot 1 of the master RSP card to slot 0 of the slave RSP card in the same router:

```
copy slot1:router-image slaveslot0:
```

Related Commands

Command	Description
boot config	Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).
boot system	Specifies the system image that the router loads at startup.
cd	Changes the default directory or file system.
copy xmodem: flash:	Copies any file from a source to a destination.
copy ymodem: flash:	Copies any file from a source to a destination.
delete	Deletes a file on a Flash memory device.
dir	Displays a list of files on a file system.
erase	Erases a file system.
ip rcmd remote-username	Configures the remote username to be used when requesting a remote copy using rcp.
reload	Reloads the operating system.
show (Flash file system)	Displays the layout and contents of a Flash memory file system.
show bootvar	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.
slave auto-sync config	Turns on automatic synchronization of configuration files for a Cisco 7507 or Cisco 7513 router that is configured for Dual RSP Backup.
verify bootflash:	Either of the identical **verify bootflash:** or **verify bootflash** commands replaces the **copy verify bootflash** command. Refer to the **verify** command for more information.

copy erase flash

The **copy erase flash** command has been replaced by the **erase flash:**command. See the description of the **erase** command for more information.

copy verify bootflash

The **copy verify bootflash** command has been replaced by the **verify bootflash:** command. See the description of the **verify** command for more information.

copy verify flash

The **copy verify flash** command has been replaced the **verify flash:** command. See the description of the **verify** command for more information.

copy verify

The **copy verify** command has been replaced by the **verify** command. See the description of the **verify** command for more information.

crypto mib topn

To configure TopN sampling parameters, use the **crypto mib topn** command in global configuration mode. To disable TopN sampling, use the **no** form of this command.

crypto mib topn [**interval** *seconds*] [**stop** *seconds*]

no crypto mib topn [**interval** *seconds*] [**stop** *seconds*]

Syntax Description

interval *seconds*	(Optional) Frequency of sampling interval, in seconds. In other words, how many minutes should pass between samples. The allowable range is from 60 to 86400 seconds (60 seconds to 24 hours). The default is 300 seconds (5 minutes). TopnMinSampleInterval: how long (in seconds) between samples? Defined in the MIB as TopnMinSampleInterval.
stop *seconds*	(Optional) Time before sampling stops, in seconds. In other words, how many minutes should pass from the time this command is executed before sampling will cease. The allowable range is from 0 to 604800 seconds. A zero (0) indicates continuous sampling. For any value other than 0, the stop time value must be greater than or equal to the sampling interval value. Defined in the MIB as TopnStopTime.

Defaults

interval: 300 seconds, **stop**: continuous sampling (0 seconds)

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use this command to rank objects according to your chosen criteria. You will not see the stop parameter setting after enabling the **show running configuration** command if the stop parameter is set at a value greater than zero. Otherwise, the current sampling parameters are recorded in the active configuration (if sampling is enabled), and sampling occurs continuously (at the specified intervals) until, and after, the device is rebooted. This command should be disabled if your criteria queries performed by XSM clients (such as VPN Device Manager [VDM]) are not to be processed.

"Crypto MIB" commands apply to characteristics of the IP Security (IPSec) MIBs. TopN (**topn**) is a special subset of the IPSec MIB Export (IPSMX) interface that provides a set of queries that allows ranked reports of active Internet Key Exchange (Ike) or IPSec tunnels to be obtained depending on certain criteria. While the VPN Device Manager (VDM) application retrieves and presents the data elements defined in the Ike and IPSec MIBs, the application does not use the SNMP interface.

Examples

The following example shows the **crypto mib topn** command being enabled with an interval frequency of 240 seconds and a designated stop time of 1200 seconds (20 minutes). At that time, the assigned sampling ceases.

```
crypto mib topn interval 240 stop 1200
```

Related Commands

Command	Description
xsm	Enables XSM client access to the router.

databits

To set the number of data bits per character that are interpreted and generated by the router hardware, use the **databits** command in line configuration mode. To restore the default value, use the **no** form of the command.

databits {**5** | **6** | **7** | **8**}

no databits

Syntax Description

5	Five data bits per character.
6	Six data bits per character.
7	Seven data bits per character.
8	Eight data bits per character. This is the default.

Defaults

Eight data bits per character

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **databits** line configuration command can be used to mask the high bit on input from devices that generate 7 data bits with parity. If parity is being generated, specify 7 data bits per character. If no parity generation is in effect, specify 8 data bits per character. The other keywords are supplied for compatibility with older devices and generally are not used.

Examples

The following example sets the number of data bits per character to seven on line 4:

```
Router(config)# line 4
Router(config-line)# databits 7
```

Related Commands

Command	Description
data-character-bits	Sets the number of data bits per character that are interpreted and generated by the Cisco IOS software.
terminal databits	Changes the number of data bits per character for the current terminal line for this session.
terminal data-character-bits	Sets the number of data bits per character that are interpreted and generated by the Cisco IOS software for the current line and session.

data-character-bits

To set the number of data bits per character that are interpreted and generated by the Cisco IOS software, use the **data-character-bits** command in line configuration mode. To restore the default value, use the **no** form of this command.

data-character-bits {**7** | **8**}

no data-character-bits

Syntax Description

7	Seven data bits per character.
8	Eight data bits per character. This is the default.

Defaults

Eight data bits per character

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **data-character-bits** line configuration command is used primarily to strip parity from X.25 connections on routers with the protocol translation software option. The **data-character-bits** line configuration command does not work on hard-wired lines.

Examples

The following example sets the number of data bits per character to seven on virtual terminal line (vty) 1:

```
Router(config)# line vty 1
Router(config-line)# data-character-bits 7
```

Related Commands

Command	Description
terminal data-character-bits	Sets the number of data bits per character that are interpreted and generated by the Cisco IOS software for the current line and session.

data-pattern

To specify the data pattern in an Service Assurance Agent (SAA) udpEcho operation to test for data corruption, use the **data pattern** command in SAA RTR configuration mode. To remove the data pattern specification, use the **no** form of this command.

data-pattern *hex-pattern*

no data-pattern *hex-pattern*

Syntax Description

hex-pattern	Hexadecimal sting to use for monitoring the specified operation.

Defaults

The default *hex-pattern* is ABCD.

Command Modes

SAA RTR configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

The **data-pattern** command allows users to specify a alphanumeric character string to verify that operation payload does not get corrupted in either direction (source-to-destination [SD] or destination-to-source [DS]).

For Cisco IOS Release 12.2(11)T, the **data-pattern** command is applicable to the udpEcho operation only. This command also applies to the Frame Relay operation in 12.2(1)T and later releases.

Examples

The following example specifies 1234ABCD5678 as the data pattern:

```
Router(config)# rtr 1
Router(config-rtr)# type udpEcho dest-ipaddr 10.0.54.205 dest-port 101
Router(config-rtr)# data-pattern 1234ABCD5678
```

Related Commands

Command	Description
show rtr collection-statistics	Displays statistical errors for all SAA operations or the specified operation.
show rtr configuration	Displays configuration values including all defaults for all SAA operations or the specified operation.

default-value exec-character-bits

To define the EXEC character width for either 7 bits or 8 bits, use the **default-value exec-character-bits** command in global configuration mode. To restore the default value, use the **no** form of this command.

default-value exec-character-bits {**7** | **8**}

no **default-value exec-character-bits**

Syntax Description

7	Selects the 7-bit ASCII character set. This is the default.
8	Selects the full 8-bit ASCII character set.

Defaults

7-bit ASCII character set

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Configuring the EXEC character width to 8 bits allows you to add graphical and international characters in banners, prompts, and so on. However, setting the EXEC character width to 8 bits can also cause failures. If a user on a terminal that is sending parity enters the **help** command, an "unrecognized command" message appears because the system is reading all 8 bits, although the eighth bit is not needed for the **help** command.

Examples

The following example selects the full 8-bit ASCII character set for EXEC banners and prompts:

```
Router(config)# default-value exec-character-bits 8
```

Related Commands

Command	Description
default-value special-character-bits	Configures the flow control default value from a 7-bit width to an 8-bit width.
exec-character-bits	Configures the character widths of EXEC and configuration command characters.
length	Sets the terminal screen length.
terminal exec-character-bits	Locally changes the ASCII character set used in EXEC and configuration command characters for the current session.
terminal special-character-bits	Changes the ASCII character widths to accept special characters for the current terminal line and session.

default-value special-character-bits

To configure the flow control default value from a 7-bit width to an 8-bit width, use the **default-value special-character-bits** command in global configuration mode. To restore the default value, use the **no** form of this command.

default-value special-character-bits {**7** | **8**}

no default-value special-character-bits

Syntax Description

7	Selects the 7-bit character set. This is the default.
8	Selects the full 8-bit character set.

Defaults

7-bit character set

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Configuring the special character width to 8 bits allows you to add graphical and international characters in banners, prompts, and so on.

Examples

The following example selects the full 8-bit special character set:

```
Router(config)# default-value special-character-bits 8
```

Related Commands

Command	Description
default-value exec-character-bits	Defines the EXEC character width for either 7 bits or 8 bits.
exec-character-bits	Configures the character widths of EXEC and configuration command characters.
length	Sets the terminal screen length.
terminal exec-character-bits	Locally changes the ASCII character set used in EXEC and configuration command characters for the current session.
terminal special-character-bits	Changes the ASCII character widths to accept special characters for the current terminal line and session.

delete

To delete a file on a Flash memory device or NVRAM, use the **delete** command in EXEC mode.

delete *url* [**/force** | **/recursive**]

Syntax Description

url	IFS URL of the file to be deleted. Include the filesystem prefix, followed by a colon, and, optionally, the name of a file or directory.
/force	(Optional) Deletes the specified file or directory with prompting you for verification. **Note** Use this keyword with caution: the system will not ask you to confirm the file deletion.
/recursive	(Optional) Deletes all files in the specified directory, as well as the directory itself.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

If you attempt to delete the configuration file or image specified by the CONFIG_FILE or BOOTLDR environment variable, the system prompts you to confirm the deletion. Also, if you attempt to delete the last valid system image specified in the BOOT environment variable, the system prompts you to confirm the deletion.

When you delete a file in Flash memory, the software simply marks the file as deleted, but it does not erase the file. To later recover a "deleted" file in Flash memory, use the **undelete** EXEC command. You can delete and undelete a file up to 15 times.

To permanently delete all files marked "deleted" on a linear Flash memory device, use the **squeeze** EXEC command.

Examples

The following example deletes the file named test from the Flash card inserted in slot 0:

```
Router# delete slot0:test
Delete slot0:test? [confirm]
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
dir	Displays a list of files on a file system.

Command	Description
show bootvar	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.
squeeze	Permanently deletes Flash files by squeezing a Class A Flash file system.
undelete	Recovers a file marked “deleted” on a Class A or Class B Flash file system.

diag

To perform field diagnostics on a line card, on the Gigabit Route Processor (GRP), on the Switch Fabric Cards (SFCs), and on the Clock Scheduler Card (CSC) in Cisco 12000 series Gigabit Switch Routers (GSRs), use the **diag** command in privileged EXEC mode. To disable field diagnostics on a line card, use the **no** form of this command.

diag *slot-number* [**halt** | **previous** | **post** | **verbose** [**wait**] | **wait**]

no diag *slot-number*

Syntax Description

slot-number	Slot number of the line card you want to test. Slot numbers range from 0 to 11 for the Cisco 12012 and 0 to 7 for the Cisco 12008 router. Slot numbers for the CSC are 16 and 17, and for the FSC are 18, 19, and 20.
halt	(Optional) Stops the field diagnostic testing on the line card.
previous	(Optional) Displays previous test results (if any) for the line card.
post	(Optional) Initiates an EPROM-based extended power-on self-test (EPOST) only. The EPOST test suite is not as comprehensive as the field diagnostics, and a pass/fail message is the only message displayed on the console.
verbose [**wait**]	(Optional) Enables the maximum status messages to be displayed on the console. By default, only the minimum status messages are displayed on the console. If you specify the optional **wait** keyword, the Cisco IOS software is not automatically reloaded on the line card after the test completes.
wait	(Optional) Stops the automatic reloading of the Cisco IOS software on the line card after the completion of the field diagnostic testing. If you use this keyword, you must use the **microcode reload** *slot* global configuration command, or manually remove and insert the line card (to power it up) in the slot so that the GRP will recognize the line card and download the Cisco IOS software image to the line card.

Defaults

No field diagnostics tests are performed on the line card.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2 GS	This command was introduced to support the Cisco 12000 series GSR.

Usage Guidelines

The **diag** command must be executed from the GRP main console port.

Perform diagnostics on the CSC only if a redundant CSC is in the router.

Diagnostics will stop and ask you for confirmation before altering the router's configuration. For example, running diagnostics on a SFC or CSC will cause the fabric to go from full bandwidth to one-fourth bandwidth. Bandwidth is not affected by GRP or line card diagnostics.

The field diagnostic software image is bundled with the Cisco IOS software and is downloaded automatically from the GRP to the target line card prior to testing.

Caution Performing field diagnostics on a line card stops all activity on the line card. Before the **diag** EXEC command begins running diagnostics, you are prompted to confirm the request to perform field diagnostics on the line card.

In normal mode, if a test fails, the title of the failed test is displayed on the console. However, not all tests that are performed are displayed. To view all the tests that are performed, use the **verbose** keyword.

After all diagnostic tests are completed on the line card, a PASSED or TEST FAILURE message is displayed. If the line card sends a PASSED message, the Cisco IOS software image on the line card is automatically reloaded unless the **wait** keyword is specified. If the line card sends a TEST FAILURE message, the Cisco IOS software image on the line card is not automatically reloaded.

If you want to reload the line card after it fails diagnostic testing, use the **microcode reload** *slot* global configuration command.

Note When you stop the field diagnostic test, the line card remains down (that is, in an unbooted state). In most cases, you stopped the testing because you need to remove the line card or replace the line card. If that is not the case, and you want to bring the line card back up (that is, online), you must use the **microcode reload** global configuration command or power cycle the line card.

If the line card fails the test, the line card is defective and should be replaced. In future releases this might not be the case because DRAM and SDRAM SIMM modules might be field replaceable units. For example, if the DRAM test failed you might only need to replace the DRAM on the line card.

For more information, refer to the Cisco 12000 series installation and configuration guides.

Examples

In the following example, a user is shown the output when field diagnostics are performed on the line card in slot 3. After the line card passes all field diagnostic tests, the Cisco IOS software is automatically reloaded on the card. Before starting the diagnostic tests, you must confirm the request to perform these tests on the line card because all activity on the line card is halted. The total/indiv. timeout set to 600/220 sec. message indicates that 600 seconds are allowed to perform all field diagnostics tests, and that no single test should exceed 220 seconds to complete.

```
Router# diag 3

Running Diags will halt ALL activity on the requested slot. [confirm]
Router#
Launching a Field Diagnostic for slot 3
Running DIAG config check
RUNNING DIAG download to slot 3 (timeout set to 400 sec.)
sending cmd FDIAG-DO ALL to fdiag in slot 3
(total/indiv. timeout set to 600/220 sec.)
Field Diagnostic ****PASSED**** for slot 3


Field Diag eeprom values: run 159 fial mode 0 (PASS) slot 3
   last test failed was 0, error code 0
sending SHUTDOWN FDIAG_QUIT to fdiag in slot 3
```

```
Board will reload
.
.
.
Router#
```

In the following example, a user is shown the output when field diagnostics are performed on the line card in slot 3 in verbose mode:

```
Router# diag 3 verbose

Running Diags will halt ALL activity on the requested slot. [confirm]
Router#
Launching a Field Diagnostic for slot 3
Running DIAG config check
RUNNING DIAG download to slot 3 (timeout set to 400 sec.)
sending cmd FDIAG-DO ALL to fdiag in slot 3
(total/indiv. timeout set to 600/220 sec.)
FDIAG_STAT_IN_PROGRESS: test #1 R5K Internal Cache
FDIAG_STAT_PASS test_num 1
FDIAG_STAT_IN_PROGRESS: test #2 Sunblock Ordering
FDIAG_STAT_PASS test_num 2
FDIAG_STAT_IN_PROGRESS: test #3 Dram Datapins
FDIAG_STAT_PASS test_num 3
.
.
.
Field Diags: FDIAG_STAT_DONE
Field Diagnostic ****PASSED**** for slot 3
Field Diag eeprom values: run 159 fial mode 0 (PASS) slot 3
   last test failed was 0, error code 0
sending SHUTDOWN FDIAG_QUIT to fdiag in slot 3

Board will reload
.
.
.
Router#
```

Related Commands

Command	Description
microcode reload	Reloads the Cisco IOS image on a line card on the Cisco 7000 series with RSP7000, Cisco 7500 series, or Cisco 12000 series routers after all microcode configuration commands have been entered.

dir

To display a list of files on a file system, use the **dir** command in EXEC mode.

dir [/**all**] [*filesystem***:**][*file-url*]

Syntax Description

/all	(Optional) Lists deleted files, undeleted files, and files with errors.
*filesystem***:**	(Optional) File system or directory containing the files to list, followed by a colon.
file-url	(Optional) The name of the files to display on a specified device. The files can be of any type. You can use wildcards in the filename. A wildcard character (*) matches all patterns. Strings after a wildcard are ignored.

Defaults

The default file system is specified by the **cd** command. When you omit the **/all** keyword, the Cisco IOS software displays only undeleted files.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.3	A timestamp that shows the offset from Coordinated Universal Time (UTC) was added to the **dir** command display.

Usage Guidelines

Use the **show** (Flash file system) command to display more detail about the files in a particular file system.

Examples

The following is sample output from the **dir** command:

```
Router# dir slot0:

Directory of slot0:/

  1  -rw-     4720148   Dec 29 2003 17:49:36  -08:00 hampton/nitro/c7200-j-mz
  2  -rw-     4767328   Jan 02 2004 18:42:53  -08:00 c7200-js-mz
  5  -rw-         639   Jan 03 2004 12:09:32  -08:00 rally
  7  -rw-         639   Jan 03 2004 12:37:13  -08:00 the_time

20578304 bytes total (3104544 bytes free)

Router# dir /all slot0:

Directory of slot0:/

  1  -rw-     4720148   Dec 15 2003 17:49:36  -08:00 hampton/nitro/c7200-j-mz
```

```
2  -rw-     4767328   Jan 02 2004 18:42:53  -08:00 c7200-js-mz
3  -rw-     7982828   Jan 02 2004 18:48:14  -08:00 [rsp-jsv-mz]
4  -rw-         639   Jan 03 2004 12:09:17  -08:00 the_time]
5  -rw-         639   Jan 03 1994 12:09:32  -08:00 rally
6  -rw-         639   Jan 03 1994 12:37:01  -08:00 [the_time]
7  -rw-         639   Jan 03 1994 12:37:13  -08:00 the_time
```

Table 20 describes the significant fields shown in the output.

Table 20 dir Field Descriptions

Field	Description
1	Index number of the file.
-rw-	Permissions. The file can be any or all of the following: • d—directory • r—readable • w—writable • x—executable
4720148	Size of the file.
Aug 29 1997 17:49:36	Last modification date.
-08:00	Conversion to local time in hours from Coordinated Universal Time (UTC). In the example, -08:00 indicates that the given time is 8 hours behind UTC or Pacific Standard Time (PST).
hampton/nitro/c7200-j-mz	Filename. Deleted files are indicated by square brackets around the filename.

Related Commands

Command	Description
cd	Changes the default directory or file system.
delete	Deletes a file on a Flash memory device.
undelete	Recovers a file marked “deleted” on a Class A or Class B Flash file system.

disable

To exit privileged EXEC mode and return to user EXEC mode, or to exit to a lower privilege level, enter the **disable** command in EXEC mode.

disable [*privilege-level*]

Syntax Description

privilege-level	(Optional) Specific privilege level (other than user EXEC mode).

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Up to 16 security levels can be configured using Cisco IOS software. If such levels are configured on a system, using this command with the *privilege-level* option allows you to exit to a lower security level. If a level is not specified, the user will exit to the user EXEC mode, which is the default.

Note Five EXEC commands are associated with privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. If you configure a privilege level greater than 0, these five commands will not be included in the command set for that privilege level.

Examples

In the following example, the user enters privileged EXEC mode using the **enable** command, then exits back to user EXEC mode using the **disable** command. Note that the prompt for user EXEC mode is >, and the prompt for privileged EXEC mode is #.

```
Router> enable
Password: <letmein>
Router# disable
Router>
```

Related Commands

Command	Description
enable	Enables higher privilege level access, such as privileged EXEC mode.

disconnect-character

To define a character to disconnect a session, use the **disconnect-character** command in line configuration mode. To remove the disconnect character, use the **no** form of this command.

disconnect-character *ascii-number*

no disconnect-character

Syntax Description

ascii-number	Decimal representation of the session disconnect character.

Defaults

No disconnect character is defined.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

See the"ASCII Character Set and Hex Values" appendix for a list of ASCII characters.

The Break character is represented by zero; NULL cannot be represented.

To use the session-disconnect character in normal communications, precede it with the escape character.

Examples

The following example defines the disconnect character for virtual terminal line 4 as Escape, which is decimal character 27:

```
Router(config)# line vty 4
Router(config-line)# disconnect-character 27
```

discover (cns)

To define the interface parameters within a Cisco Networking Services (CNS) connect profile for connecting to the CNS configuration engine, use the **discover** command in CNS connect configuration mode. To disable this functionality, use the **no** form of this command.

discover {**line** *line-type* | **controller** *controller-type* | **interface** [*interface-type*] | **dlci** [**subinterface** *subinterface-number*]}

no discover {**line** *line-type* | **controller** *controller-type* | **interface** [*interface-type*] | **dlci** [**subinterface** *subinterface-number*]}

Syntax Description

line *line-type*	Line type to be used for connecting to the CNS configuration engine. When the **line** *line-type* keyword and argument are specified, all the lines that create an interface that match the specified *line-type* argument are discovered. The CNS connect templates associated with the **discover line** *line-type* command are applied in line configuration mode.
controller *controller-type*	Controller type to be used for connecting to the CNS configuration engine. When the **controller** *controller-type* keyword and argument are specified, all the controllers that create an interface that match the specified *controller-type* argument are discovered. The CNS connect templates associated with the **discover controller** *controller-type* command are applied in controller configuration mode.
interface [*interface-type*]	Interface type to be used for connecting to the CNS configuration engine. If the **discover interface** *interface-type* command is the first **discover** command configured in a CNS connect profile, then the interfaces that match the specified *interface-type* argument are discovered. If the **discover interface** *interface-type* command is configured after the **discover line** *line-type* or **discover controller** *controller-type* commands in a CNS connect profile, then the specified *interface-type* argument is ignored. Instead, the CNS connect templates associated with the **discover interface** command are applied to all the interfaces associated with the preceding **discover line** *line-type* or **discover controller** *controller-type* commands. The CNS connect templates associated with the **discover interface** *interface-type* command are applied in interface configuration mode.

dlci	Active DLCIs to be used for connecting to the CNS configuration engine. When this keyword is defined, all the active DLCIs are discovered on the interface specified by the preceding **discover interface** *interface-type* command. A Frame Relay LMI message will return a list of active DLCIs. Active DLCIs can only be discovered on interfaces configured with Frame Relay. Therefore, the location of the **discover dlci** command in a CNS connect profile is important. It must be entered after the interfaces have been configured with Frame Relay. The CNS connect templates associated with the **discover dlci** command are applied in subinterface (point-to-point) configuration mode. Defines the CNS connect variable **${dlci}** and **${next-hop}**. **Note** Any Cisco IOS command that requires knowledge of the active DLCIs must be configured after the **discover dlci** command.
subinterface *subinterface-number*	(Optional) Point-to-point subinterface number used to perform a search for active DLCIs. If the number is not specified, the default value is 9999.

Defaults

No interface parameters within a CNS connect profile are defined.

Command Modes

CNS connect configuration

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.3(9)	This command was integrated into Cisco IOS Release 12.3(9). The **dlci subinterface** *subinterface-number* keywords and argument, and the CNS connect variable **${dlci}** are not supported in this release.

Usage Guidelines

First use the **cns connect** command to enter CNS connect configuration mode and define the parameters of a CNS connect profile for connecting to the CNS configuration engine. Then use the following CNS connect commands to create a CNS connect profile:

- **discover**
- **template**

A CNS connect profile specifies the **discover** commands and associated **template** commands that are to be applied to a router's configuration. The first **discover** command in a CNS connect profile defines the scope of the interfaces for which to search and use to perform the ping iterations for connecting to the CNS configuration engine. Subsequent **discover** commands limit this scope. The search is based on discovering all the interfaces that match the specified line, controller, or interface type. The search is case-insensitive and allows for abbreviations. For example, the **discover interface Serial**, **discover interface Ser**, **discover interface serial**, and **discover interface ser** commands all match the serial interface.

Each **discover** command must have at least one unique CNS connect template associated with it. Specifically, the **template** command must be configured after configuring the **discover** command. The **discover** command specifies the configuration mode in which the CNS connect templates (specified by the **template** command that is associated with the **discover** command) are to be applied. When multiple **discover** and **template** commands are configured in a CNS connect profile, they are processed in the order in which they are entered.

Table 21 provides a summary of the interface parameters that can be defined using the **discover** command.

Table 21 Summary of the discover Commands

discover Command	Description	Associated CNS Connect Variable	Configuration Mode in Which CNS Connect Templates Are Applied	Prerequisite discover Command	Required Subsequent discover Command
discover line *line-type*	Discovers all the lines that create an interface that match the specified *line-type* argument.	**${line}**	Line	—	**discover interface** *interface-type*
discover controller *controller-type*	Discovers all the controllers that create an interface that match the specified *controller-type* argument.	**${controller}**	Controller	—	**discover interface** *interface-type*
discover interface [*interface-type*]	• If this is the first **discover** command configured, then all the interfaces that match the specified *interface-type* argument are discovered. • If configured after the **discover line** *line-type* or **discover controller** *controller-type* commands, then the specified *interface-type* argument is ignored.	**${interface}** **${next-hop}**	Interface	—	—
discover dlci [**subinterface** *subinterface-number*]	Discovers all active DLCIs on the interface specified by the preceding **discover interface** command.	**${dlci}** **${next-hop}**	Subinterface (point-to-point)	**discover interface** *interface-type*	—

CNS connect variables can be used as placeholders within a CNS connect template configuration. Each variable is defined by an associated **discover** command (see Table 21 and Table 22). Before a CNS connect template that contains these variables is applied to a router's configuration, the variables are replaced by the values defined by their associated **discover** command. For example, if the **discover interface serial** command was configured, and you were able to connect to the CNS configuration engine using Serial0/0, then the **cli ip route 0.0.0.0 0.0.0.0 ${interface}** command would generate the **cli ip route 0.0.0.0 0.0.0.0 serial0/0** command.

Table 22 Summary of the CNS Connect Variables

Variable	Description
${line}	The line type defined by the associated **discover line** *line-type* command.
${controller}	The controller type defined by the associated **discover controller** *controller-type* command.
${interface}	The interface type defined by the associated **discover interface** command.
${dlci}	The active DLCI defined by the associated **discover dlci** command.
${next-hop}	The next hop interface. This variable is identical to the **${interface}** variable unless the **discover dlci** command has been configured. In this case, the **${next-hop}** variable is identical to the **${interface}.{subinterface}** variable, where the **{subinterface}** variable is specified by the **discover dlci** command. The **${next-hop}** variable should only be used in the CNS connect templates after the last **discover** command has been entered. A typical use of this variable is to allow the default IP route to be configured to send traffic towards the CNS configuration engine. Note that the CNS configuration engine may not be on the same LAN as the router. Therefore, configuring a route to the CNS configuration engine may require deployment-specific knowledge. Common practice is to define a default route to the interface using the **ip route** command (for example, **cli ip route 0.0.0.0 0.0.0.0 ${next-hop}**).
$$	A literal substitution of the $ symbol.

Note Effective with Cisco IOS Releases 12.3(8)T and 12.3(9), the **&** variable is replaced by the **${interface}** variable.

Examples

The following example shows how to create a CNS connect profile named EG:

```
Router (config)# cns connect EG
Router (config-cns-conn)# discover controller T1
Router (config-cns-conn)# template timeslot-1
Router (config-cns-conn)# discover interface
Router (config-cns-conn)# template frame
Router (config-cns-conn)# exit
Router (config)#
```

In this example, the following sequence of events occur for each T1 controller when the **cns connect EG** command is processed:

1. Enter controller configuration mode and apply all commands in the timeslot-1 template to the router's configuration.
2. For each interface associated with each T1 controller:
   a. Enter interface configuration mode and apply all commands in the frame template to the router's configuration.
   b. Try to ping the CNS configuration engine.

c. If the ping is successful, then download pertinent configuration information from the CNS configuration engine and exit. The **cns connect EG** command has completed its process.

d. If the ping is unsuccessful, enter interface configuration mode and remove all commands in the frame template from the router's configuration.

3. Enter controller configuration mode and remove all commands in the timeslot-1 template from the router's configuration. The **cns connect EG** command has failed to retrieve any configuration information from the CNS configuration engine.

Related Commands

Command	Description
cli (cns)	Specifies the command lines of a CNS connect template.
cns connect	Enters CNS connect configuration mode and defines the parameters of a CNS connect profile for connecting to the CNS configuration engine.
cns template connect	Enters CNS template connect configuration mode and defines the name of a CNS connect template.
template (cns)	Specifies a list of CNS connect templates within a CNS connect profile to be applied to a router's configuration.

dispatch-character

To define a character that causes a packet to be sent, use the **dispatch-character** command in line configuration mode. To remove the definition of the specified dispatch character, use the **no** form of this command.

dispatch-character *ascii-number1* [*ascii-number2 . . . ascii-number*]

no dispatch-character *ascii-number1* [*ascii-number2 . . . ascii-number*]

Syntax Description

ascii-number1	Decimal representation of the desired dispatch character.
ascii-number2 . . . ascii-number	(Optional) Additional decimal representations of characters. This syntax indicates that you can define any number of characters as dispatch characters.

Defaults

No dispatch character is defined.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

See the "ASCII Character Set and Hex Values" appendix for a list of ASCII characters.

The **dispatch-character** command defines one or more dispatch characters that cause a packet to be sent even if the dispatch timer has not expired. Use of a dispatch character causes the Cisco IOS software to attempt to buffer characters into larger-sized packets for transmission to the remote host.

Enable the **dispatch-character** command from the session that initiates the connection, not from the incoming side of a streaming Telnet session.

This command can take multiple arguments, so you can define any number of characters as dispatch characters.

Examples

The following example defines the Return character (decimal 13) as the dispatch character for virtual terminal line (vty) line 4:

```
Router(config)# line vty 4
Router(config-line)# dispatch-character 13
```

Related Commands

Command	Description
dispatch-machine	Specifies an identifier for a TCP packet dispatch state machine on a particular line.
dispatch-timeout	Sets the character dispatch timer.
state-machine	Specifies the transition criteria for the state of a particular state machine.
terminal dispatch-character	Defines a character that causes a packet to be sent for the current session.

dispatch-machine

To specify an identifier for a TCP packet dispatch state machine on a particular line, use the **dispatch-machine** command in line configuration mode. To disable a state machine on a particular line, use the **no** form of this command.

dispatch-machine *name*

no dispatch-machine

Syntax Description

name	Name of the state machine that determines when to send packets on the asynchronous line.

Defaults

No dispatch state machine identifier is defined.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When the **dispatch-timeout** command is specified, a packet being built will be sent when the timer expires, and the state will be reset to zero.

Any dispatch characters specified using the **dispatch-character** command are ignored when a state machine is also specified.

If a packet becomes full, it will be sent regardless of the current state, but the state will not be reset. The packet size depends on the traffic level on the asynchronous line and the dispatch-timeout value. There is always room for 60 data bytes. If the dispatch-timeout value is greater than or equal to 100 milliseconds, a packet size of 536 (data bytes) is allocated.

Examples

The following example specifies the name linefeed for the state machine:

```
Router(config)# state-machine linefeed 0 0 9 0
Router(config)# state-machine linefeed 0 11 255 0
Router(config)# state-machine linefeed 0 10 10 transmit
Router(config)# line 1
Router(config-line)# dispatch-machine linefeed
```

Related Commands

Command	Description
dispatch-character	Defines a character that causes a packet to be sent.
dispatch-timeout	Sets the character dispatch timer.
state-machine	Specifies the transition criteria for the state of a particular state machine.

dispatch-timeout

To set the character dispatch timer, use the **dispatch-timeout** command in line configuration mode. To remove the timeout definition, use the **no** form of this command.

dispatch-timeout *milliseconds*

no dispatch-timeout

Syntax Description

milliseconds	Integer that specifies the number of milliseconds (ms) that the Cisco IOS software waits after putting the first character into a packet buffer before sending the packet. During this interval, more characters can be added to the packet, which increases the processing efficiency of the remote host.

Defaults

No dispatch timeout is defined.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command to increase the processing efficiency for the remote host.

The **dispatch-timeout** line configuration command causes the software to buffer characters into packets for transmission to the remote host. The Cisco IOS software sends a packet a specified amount of time after the first character is put into the buffer. You can use the **dispatch-timeout** and **dispatch-character** line configuration commands together. In this case, the software dispatches a packet each time the dispatch character is entered, or after the specified dispatch timeout interval, depending on which condition is met first.

Note The system response time might appear intermittent if the timeout interval is greater than 100 milliseconds and remote echoing is used. For lines with a reverse-Telnet connection, use a dispatch-timeout value less than 10 milliseconds.

Examples

The following example sets the dispatch timer to 80 milliseconds for virtual terminal line (vty) lines 0 through 4:

```
Router(config)# line vty 0 4
Router(config-line)# dispatch-timeout 80
```

Related Commands

Command	Description
dispatch-character	Defines a character that causes a packet to be sent.
dispatch-machine	Specifies an identifier for a TCP packet dispatch state machine on a particular line.
state-machine	Specifies the transition criteria for the state of a particular state machine.
terminal dispatch-timeout	Sets the character dispatch timer for the current session.

distributions-of-statistics-kept

To set the number of statistic distributions kept per hop during a SSA operation, use the **distributions-of-statistics-kept** command in SAA RTR configuration mode. To return to the default value, use the **no** form of this command.

distributions-of-statistics-kept *size*

no distributions-of-statistics-kept

Syntax Description

size	Number of statistic distributions kept per hop. The default is 1 distribution.

Defaults

1 distribution

Command Modes

SAA RTR configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

In most situations, you do not need to change the statistic distribution size for the SAA. Only change the size when distributions are needed (for example, when performing statistical modeling of your network).

Note Increasing the distributions also increases the RAM usage. The total number of statistics distributions captured will be: the value of **distributions-of-statistics-kept** times the value of **hops-of-statistics-kept** times the value of **paths-of-statistics-kept** times the value of **hours-of-statistics-kept**.

When the number of distributions reaches the size specified, no further distribution information is stored.

Examples

The following example sets the distribution to 5 and the distribution interval to 10 ms. This setting means that the first distribution will contain statistics from 0 to 9 ms, the second distribution will contain statistics from 10 to 19 ms, the third distribution will contain statistics from 20 to 29 ms, the fourth distribution will contain statistics from 30 to 39 ms, and the fifth distribution will contain statistics from 40 ms to infinity.

```
Router(config)# rtr 1
Router(config-rtr)# type echo protocol ipIcmpEcho 172.16.161.21
Router(config-rtr)# distributions-of-statistics-kept 5
Router(config-rtr)# statistics-distribution-interval 10
```

Related Commands

Command	Description
hops-of-statistics-kept	Sets the number of hops for which statistics are maintained per path for the SAA operation.
hours-of-statistics-kept	Sets the number of hours for which statistics are maintained for the SAA operation.
paths-of-statistics-kept	Sets the number of paths for which statistics are maintained per hour for the SAA operation.
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.
statistics-distribution-interval	Sets the time interval for each statistics distribution kept for SAA.

do

To execute an EXEC-level command from global configuration mode or any configuration submode, use the **do** command in any configuration mode.

do *command*

Syntax Description

command	The EXEC command to be executed.

Defaults

No default behavior or values.

Command Modes

All configuration modes

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Use this command to execute EXEC commands (such as **show**, **clear**, and **debug** commands) while configuring your routing device. After the EXEC command is executed, the system will return to the configuration mode you were using.

Tip This command can be useful for saving your configuration to the startup-config file without having to return to the EXEC mode (**do copy running-config startup-config**), or for checking the status of a feature (using a **do show** command) while configuring the feature.

Examples

In the following example, the **show interfaces** EXEC command is issued from within global configuration mode:

```
Router(config)# do show interfaces serial 3/0

Serial3/0 is up, line protocol is up
  Hardware is M8T-RS232
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output 1d17h, output hang never
  Last clearing of "show interface" counters never
.
.
.
Router(config)#
```

In the following example, the **clear vpdn tunnel** EXEC command is issued from within VPDN configuration mode:

```
Router(config-vpdn)# do clear vpdn tunnel
Router(config-vpdn)#
```

downward-compatible-config

To generate a configuration that is compatible with an earlier Cisco IOS release, use the **downward-compatible-config** command in global configuration mode. To disable this function, use the **no** form of this command.

downward-compatible-config *version*

no downward-compatible-config

Syntax Description

version	Cisco IOS release number, not earlier than Release 10.2.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

In Cisco IOS Release 10.3, IP access lists changed format. Use the **downward-compatible-config** command to regenerate a configuration in a format prior to Release 10.3 if you are going to downgrade from your software version to version 10.2 or 10.3. The earliest *version* value this command accepts is 10.2.

When this command is configured, the router attempts to generate a configuration that is compatible with the specified version. Note that this command affects only IP access lists.

Under some circumstances, the software might not be able to generate a fully backward-compatible configuration. In such a case, the software issues a warning message.

Examples

The following example generates a configuration file compatible with Cisco IOS Release 10.2 access lists:

```
Router(config)# downward-compatible-config 10.2
```

Related Commands

Command	Description
access-list (extended)	Provides extended access lists that allow more detailed access lists.
access-list (standard)	Defines a standard XNS access list.

editing

To reenable Cisco IOS enhanced editing features for a particular line after they have been disabled, use the **editing** command in line configuration mode. To disable these features, use the **no** form of this command.

editing

no editing

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Enhanced editing features are enabled by default. However, there may be situations in which you need to disable these features. The **no** form of this command disables these enhanced editing features, and the plain form of the command can be used to reenable these features.

Table 23 provides a description of the keys used to enter and edit commands when the editing features are enabled. Ctrl indicates the Control key, which must be pressed simultaneously with its associated letter key. Esc indicates the Escape key, which must be pressed first, followed by its associated letter key. A comma is used in the following table to indicate a key sequence (the comma key should not be pressed). Keys are not case sensitive. Many letters used for CLI navigation and editing were chosen to provide an easy way of remembering their functions. In the following table (Table 23), characters are bolded in the “Function Summary” column to indicate the relation between the letter used and the function.

Table 23 Command Editing Keys and Functions

Keys	Function Summary	Function Details
Tab	Complete command	Completes a partial command name entry. When you enter a unique set of characters and press the Tab key, the system completes the command name. If you enter a set of characters that could indicate more than one command, the system beeps to indicate an error. To view the commands which match the set of characters you have entered, enter a question mark (?) immediately following the partial command (no space). The CLI will then list the commands that begin with that string.
Return (at the command line)	Execute	Executes the command.
Return (at the --More-- prompt)	Continue	Displays the next line of output.
Space Bar (at the --More-- prompt)	Continue	Displays the next screen of output. The amount of output you see will depend on the screen depth setting of your terminal.
Delete or Backspace	Backspace	Erases the character to the left of the cursor.
Left Arrow[1] or Ctrl-B	**B**ack character	Moves the cursor one character to the left. When you enter a command that extends beyond a single line, you can press the Left Arrow or Ctrl-B keys repeatedly to scroll back toward the system prompt and verify the beginning of the command entry.
Right Arrow[1] or Ctrl-F	**F**orward character	Moves the cursor one character to the right.
Esc, B	**B**ack word	Moves the cursor back one word.
Esc, F	**F**orward word	Moves the cursor forward one word.
Ctrl-A	Beginning of line	Moves the cursor to the beginning of the line.
Ctrl-E	**E**nd of line	Moves the cursor to the end of the command line.
Ctrl-D	**D**elete character	Deletes the character at the cursor.
Esc, D	**D**elete next word	Deletes from the cursor to the end of the word.
Ctrl-W	Delete previous **w**ord	Deletes the word to the left of the cursor.
Ctrl-K	Delete line forward	Deletes all characters from the cursor to the end of the command line.
Ctrl-U or Ctrl-X	Delete line backward	Deletes all characters from the cursor back to the beginning of the command line.
Ctrl-T	**T**ranspose characters	Transposes the character to the left of the cursor with the character located at the cursor.

Table 23 Command Editing Keys and Functions (continued)

Keys	Function Summary	Function Details
Ctrl-R or Ctrl-L	**R**edisplay **l**ine	Redisplays the system prompt and command line.
Ctrl-V or Esc, Q	Ignore editing	Inserts a code to indicate to the system that the keystroke immediately following should be treated as a command entry, *not* as an editing key.
Up Arrow[1] or Ctrl-P	**P**revious command	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Down Arrow[1] or Ctrl-N (next)	**N**ext command	Returns to more recent commands in the history buffer (after recalling commands with the Up Arrow or Ctrl-P). Repeat the key sequence to recall successively more recent commands.
Ctrl-Y	Recall last deleted command	Recalls the most recent entry in the delete buffer. The delete buffer contains the last ten items you have deleted or cut. Ctrl-Y can be used in conjunction with Esc Y.
Esc, Y	Recall next deleted command	Recalls the next entry in the delete buffer. The delete buffer contains the last ten items you have deleted. Press Ctrl-Y first to recall the most recent entry. Then press Esc Y up to nine times to recall the remaining entries in the buffer. If you bypass an entry, continue to press Esc Y to cycle back to it.
Esc, C	**C**apitalize word	Capitalizes the word from the cursor to the end of the word.
Esc, U	Make word **u**ppercase	Changes all letters from the cursor to the next space on the line appear in uppercase letters.
Esc, L	Make word **l**owercase	Changes the word to lowercase from the cursor to the end of the word.

1. The arrow keys function only with ANSI-compatible terminals.

Examples

In the following example, enhanced editing mode is disabled on line 3:

```
Router(config)# line 3
Router(config-line)# no editing
```

Related Commands

Command	Description
terminal editing	Controls CLI enhanced editing feature for the current terminal session.

enable

To enter privileged EXEC mode, or any other security level set by a system administrator, use the **enable** command in EXEC mode.

enable [*privilege-level*]

Syntax Description

privilege-level	(Optional) Privilege level at which to log in.

Defaults

Privilege-level 15 (privileged EXEC)

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Entering privileged EXEC mode enables the use of privileged commands. Because many of the privileged commands set operating parameters, privileged access should be password-protected to prevent unauthorized use. If the system administrator has set a password with the **enable password** global configuration command, you are prompted to enter it before being allowed access to privileged EXEC mode. The password is case sensitive.

If an **enable** password has not been set, enable mode only can be accessed through the console connection.

Security levels can be set by an administrator using the **enable password** and **privilege level** commands. Up to 16 privilege levels can be specified, using the numbers 0 through 15. Using these privilege levels, the administrator can allow or deny access to specific commands. Privilege level 0 is associated with user EXEC mode, and privilege level 15 is associated with privileged EXEC mode.

For more information on defined privilege levels, see the *Cisco IOS Security Configuration Guide* and the *Cisco IOS Security Command Reference* publications.

If a level is not specified when entering the **enable** command, the user will enter the default mode of privileged EXEC (level 15).

Examples

In the following example, the user enters privileged EXEC mode using the **enable** command. The system prompts the user for a password before allowing access to the privileged EXEC mode. The password is not printed to the screen. The user then exits back to user EXEC mode using the **disable** command. Note that the prompt for user EXEC mode is >, and the prompt for privileged EXEC mode is #.

```
Router> enable
Password: <letmein>
Router# disable
Router>
```

Related Commands

Command	Description
disable	Exits from privileged EXEC mode to user EXEC mode, or, if privilege levels are set, to the specified privilege level.
enable password	Sets a local password to control access to various privilege levels.
privilege level (global)	Sets a privilege level for a command.
privilege level (line)	Sets a privilege level for a command for a specific line.

end

To end the current configuration session and return to privileged EXEC mode, use the **end** command in global configuration mode.

end

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command will bring you back to privileged EXEC mode regardless of what configuration mode or configuration submode you are in.

Note This global configuration command can be used in any configuration mode.

Use this command when you are done configuring the system and you want to return to EXEC mode to perform verification steps.

Examples

In the following example, the **end** command is used to exit from ALPS ASCU configuration mode and return to privileged EXEC mode. A **show** command is used in privileged EXEC mode to verify the configuration.

```
Router# configure terminal
Router(config)# interface serial 1:1
Router(config-if)# alps ascu 4B
Router(config-alps-ascu)# end
Router# show interface serial 1:1
```

Related Commands

Command	Description
exit (global)	Exits from the current configuration mode.

enhanced-history

To enable enhanced history gathering for an Service Assurance Agent (SAA) operation, use the **enhanced-history** command in one of the SAA RTR configuration modes.

enhanced-history interval *seconds* **buckets** *number-of-buckets*

Syntax Description

interval *seconds*	The number of seconds enhanced history should be gathered in each bucket. When this time expires, enhanced history statistics are gathered in a new bucket. The default is 900 seconds (15 minutes).
buckets *number-of-buckets*	The number of history buckets that should be retained in system memory. When this number is reached, statistic gathering for the operation ends. The default is 100 buckets.

Defaults

For SLM operations, 900 seconds and 100 buckets

Command Modes

SAA Echo operation configuration (config-rtr-echo)

SAA UDP Echo operation configuration (config-rtr-udp)

SAA TCP operation configuration (config-rtr-tcp)

SAA Jitter operation configuration (config-rtr-jitter)

SAA SLM Controller/Interface configuration (config-rtr-slm-if)

SAA SLM ATM Interface configuration (config-rtr-slm-atm-if)

SAA SLM Frame Relay Interface configuration (config-rtr-slm-fr-if)

SAA SLM ATM Circuit configuration (config-rtr-slm-atm-dlci)

SAA SLM Frame Relay Circuit configuration (config-rtr-slm-fr-dlci)

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.3(1)	This command was made available for SAA SLM Frame Relay configuration modes.

Usage Guidelines

Performance statistics are stored in "buckets" which keep the accumulated data separate from each other. Each bucket consists of data accumulated over the specified interval. For Frame Relay SLM and ATM SLM operations, each bucket consists of 15 minutes (900 seconds) worth of statistics. The following line will be written to the configuration:

```
enhanced-history interval 900 buckets 100
```

Regardless of the values entered for *seconds* and *number-of-buckets*, the default of value of a 900-second interval and 100 history buckets will be used. Your input is overridden in the Frame Relay operations so that complete SLM statistics can be provided.

Examples

In the following example SAA operation 3 is configured with the standard enhanced history characteristics:

```
Router(config)# rtr slm frame-relay statistics
Router(config)# rtr 3
Router(config-rtr)# type slm frame-relay pvc interface Serial0:0 111
Router(config-rtr-slm-fr-dlci)# enhanced-history interval 900 buckets 100
Router(config-rtr-slm-fr-dlci)# exit
Router(config)# rtr schedule 3 start-time now life forever
Router(config)# end
Router#
```

Related Commands

Command	Description
type slm controller	Specifies that the SAA operation is an SLM controller operation, and specifies the controller that the operation should be run on.
type slm frame-relay interface	Specifies that the SAA operation is an SLM FR interface operation, and specifies the interface that the operation should be run on.
type slm frame-relay pvc interface	Specifies that the SAA operation is an SLM FR circuit operation, and specifies the interface and DLCI number that the operation should be run on.
type slm interface	Specifies that the SAA operation is an SLM interface operation, and specifies the interface that the operation should be run on.

erase

To erase a file system, use the **erase** command in EXEC mode.

erase [**/no-squeeze**] *filesystem***:**

Syntax Description

/no-squeeze	Disables the squeeze operation to conserve memory and makes the **erase** option compatible with older filesystems.
*filesystem***:**	File system name, followed by a colon. For example, **flash:** or **nvram:**

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(11)T	The **/no-squeeze** option was added for the Cisco 1700 series.

Usage Guidelines

The **erase nvram:** command replaces the **write erase** command and the **erase startup-config** command.

When a file system is erased, none of the files in the file system can be recovered.

The **erase** command can be used on both Class B and Class C Flash file systems only. To reclaim space on Flash file systems after deleting files using the **delete** command, you must use the **erase** command. This command erases all of the files in the Flash file system.

If the flash memory is partitioned, all partitions must be removed before using the **erase** command.

Class A Flash file systems cannot be erased. You can delete individual files using the **delete** EXEC command and then reclaim the space using the **squeeze** EXEC command. You can use the **format** EXEC command to format the Flash file system.

On Class C Flash file systems, space is dynamically reclaimed when you use the **delete** command. You can also use either the **format** or **erase** command to reinstalled a Class C Flash file system.

The **erase nvram:** command erases NVRAM. On Class A file system platforms, if the CONFIG_FILE variable specifies a file in Flash memory, the specified file will be marked “deleted.”

The **/no-squeeze** option is available on systems with small amounts of Flash memory in order to conserve memory. When a squeeze operation is performed, the last two erase sectors are permanently reservered for the squeeze logs and squeeze buffer. Disabling the squeeze operation keeps these memory sectors free. If any sectors using squeeze data are detected, they will be erased when this option is used.

Examples

The following example erases the NVRAM, including the startup configuration located there:

```
erase nvram:
```

The following example erases all of partition 2 in internal Flash memory:

```
Router# erase flash:2

System flash directory, partition 2:
File  Length   Name/status
  1   1711088  dirt/images/c3600-i-mz
[1711152 bytes used, 15066064 available, 16777216 total]

Erase flash device, partition 2? [confirm]
Are you sure? [yes/no]: yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
```

The following example erases Flash memory when Flash is partitioned, but no partition is specified in the command:

```
Router# erase flash:

System flash partition information:
Partition   Size     Used    Free    Bank-Size   State       Copy-Mode
    1       4096K    2048K   2048K   2048K       Read Only   RXBOOT-FLH
    2       4096K    2048K   2048K   2048K       Read/Write  Direct

[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 2]
```

The system will prompt only if there are two or more read/write partitions. If the partition entered is not valid or is the read-only partition, the process terminates. You can enter a partition number, a question mark (**?**) for a directory display of all partitions, or a question mark and a number (**?***number*) for directory display of a particular partition. The default is the first read/write partition.

```
System flash directory, partition 2:
File  Length   Name/status
  1   3459720  master/igs-bfpx.100-4.3
[3459784 bytes used, 734520 available, 4194304 total]

Erase flash device, partition 2? [confirm] <Return>
```

Related Commands

Command	Description
boot config	Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).
delete	Deletes a file on a Flash memory device.
more nvram:startup-config	Displays the startup configuration file contained in NVRAM or specified by the CONFIG_FILE environment variable.
show bootvar	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.
undelete	Recovers a file marked “deleted” on a Class A or Class B Flash file system.

erase bootflash

The **erase bootflash:** and **erase bootflash** commands have identical functions. See the description of the **erase** command in this chapter for more information.

escape-character

To define a system escape character, use the **escape-character** command in line configuration mode. To set the escape character to Break, use the **no** or **default** form of this command.

escape-character {*ascii-number* | *character* | **break** | **default** | **none**} [**soft**]

no escape-character [**soft**]

default escape-character

Syntax Description

ascii-number	ASCII decimal representation of a character or a control sequence (for example, Ctrl-E) to be used as the escape character.
character	Character to be used as the escape character (for example, **!**).
break	Sets the escape character to Break. Note that the Break key should not be used as an escape character on a console terminal.
default	Sets the escape key sequence to the default of Ctrl-^, X.
none	Disables escape entirely.
soft	(Optional) Sets an escape character that will wait until pending input is processed before it executes.

Defaults

The default escape key sequence is Ctrl-Shift-6 (Ctrl-^) or Ctrl-Shift-6, X (^^X). The X is generally only required for modem connections.

The **default escape-character** command sets the escape character to Break (the default setting for Break is Ctrl-C).

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
11.3	The **soft** keyword was added.

Usage Guidelines

See the "ASCII Character Set and Hexidecimal Values" appendix for a list of ASCII characters.

The escape character (or key sequence) suspends any actively running processes and returns you to privileged EXEC mode or, if a menu is being used, to the system menu interface. The escape character is used for interrupting or aborting a process started by previously executed command. Examples of processes from which you can escape include Domain-Name lookup, **ping**, **trace**, and Telnet sessions initiated from the device to which you are connected.

To view the current setting of the escape sequence for a line, use the **show line** command followed by the specific line identifier (for example, **show line 0**, or **show line console**). The default escape sequence for a line is often displayed as ^^X . The first caret symbol represents the Control (Ctrl) key, the second caret symbol is literal (Shift-6), and the X is literal (for most systems, the X is not required).

To set the escape key for the active terminal line session, use the **terminal escape-character** command.

The Break key cannot be used as an escape character on a console terminal because the Cisco IOS software interprets Break as an instruction to halt the system. Depending upon the configuration register setting, break commands issued from the console line either will be ignored or cause the server to shut down.

To send an escape sequence over a Telnet connection, press **Ctrl-Shift-6** twice.

The **escape-character soft** form of this command defines a character or character sequence that will cause the system to wait until pending input is processed before suspending the current session. This option allows you to program a key sequence to perform multiple actions, such as using the F1 key to execute a command, then execute the escape function after the first command is executed.

The following restrictions apply when using the **soft** keyword:

- The length of the logout sequence must be 14 characters or fewer.
- The soft escape character cannot be the same as the generic Cisco escape character, Break, or the characters b, d, n, or s.
- The soft escape character should be an ASCII value from 1 to 127. Do not use the number 30.

Examples

The following example sets the escape character for the console line to the keyboard entry Ctrl-P, which is represented by the ASCII decimal value of 16:

```
Router(config)# line console
Router(config-line)# escape-character 16
```

The following example sets the escape character for line 1 to **!**, which is represented in the configuration file as the ASCII number 33:

```
Router(config)# line 1
Router(config-line)# escape-character !
Router(config-line)# end
Router# show running-config
Building configuration...
.
.
.
line 1
 autoselect during-login
 autoselect ppp
 modem InOut
 transport preferred none
 transport output telnet
 escape-character 33
.
.
.
```

Related Commands

Command	Description
show line	Displays information about the specified line connection, or all the lines.
terminal escape-character	Sets the escape character for the current terminal line for the current session.

exception core-file

To specify the name of the core dump file, use the **exception core-file** command in global configuration mode. To return to the default core filename, use the **no** form of this command.

exception core-file *filename*

no exception core-file

Syntax Description

filename	Name of the core dump file saved on the server.

Defaults

The core file is named *hostname*-core, where *hostname* is the name of the router.

Command Modes

Global configuration

Command History

Release	Modification
10.2	This command was introduced.

Usage Guidelines

If you use TFTP to dump the core file to a server, the router will only dump the first 16 MB of the core file. If the router's memory is larger than 16 MB, the whole core file will not be copied to the server. Therefore, use rcp or FTP to dump the core file.

Caution Use the **exception** commands only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, FTP, or rcp server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

Examples

In the following example, the router is configured to use FTP to dump a core file named dumpfile to the FTP server at 172.17.92.2 when it crashes:

```
Router(config)# ip ftp username red
Router(config)# ip ftp password blue
Router(config)# exception protocol ftp
Router(config)# exception dump 172.17.92.2
Router(config)# exception core-file dumpfile
```

Related Commands

Command	Description
exception dump	Causes the router to dump a core file to a particular server when the router crashes.
exception memory	Causes the router to create a core dump and reboot when certain memory size parameters are violated.

Command	Description
exception protocol	Configures the protocol used for core dumps.
exception spurious-interrupt	Causes the router to create a core dump and reload after a specified number of spurious interrupts.
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp username	Configures the username for FTP connections.

exception crashinfo buffersize

To change the size of the buffer used for crashinfo files, use the **exception crashinfo buffersize** command in global configuration mode. To revert to the default buffersize, use the **no** form of this command.

exception crashinfo buffersize *kilobytes*

no exception crashinfo buffersize *kilobytes*

Syntax Description

kilobytes	Sets the size of the buffersize to the specified value within the range of 32 to 100 kilobytes. The default is 32KB.

Defaults

Crashinfo buffer is 32KB.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T, 12.2(11)	This command was introduced for the Cisco 3600 series only (3620, 2640, and 3660 platforms).
12.2(13)T	This command was implemented in 6400-NSP images.

Usage Guidelines

The crashinfo file saves information that helps Cisco technical support representatives to debug problems that caused the Cisco IOS image to fail (crash). The switch writes the crash information to the console at the time of the failure, and the file is created the next time you boot the Cisco IOS image after the failure (instead of while the system is failing).

Examples

In the following example, the crashinfo buffer is set to 100 KB:

```
Router(config)# exception crashinfo buffersize 100
```

Related Commands

Command	Description
exception crashinfo file	Enables the creation of a diagnostic file at the time of unexpected system shutdowns.

exception crashinfo file

To enable the creation of a diagnostic file at the time of unexpected system shutdowns, use the **exception crashinfo file** command in global configuration mode. To disable the creation of crashinfo files, use the **no** form of this command.

exception crashinfo file *device*:*filename*

no exception crashinfo file *device*:*filename*

Syntax Description

device:filename	Specifies the flash device and file name to be used for storing the diagnostic information. The colon is required.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T, 12.2(11)	This command was introduced for the Cisco 3600 series only.
12.2(13)T	This command was implemented in 6400-NSP images.

Usage Guidelines

The "crashinfo" file saves information that helps Cisco technical support representatives to debug problems that caused the Cisco IOS image to fail (crash). The switch writes the crash information to the console at the time of the failure, and the file is created the next time you boot the IOS image after the failure (instead of while the system is failing). The filename will be *filename_yyyymmdd-hhmmss*, where *y* is year, *m* is month, *d* is date, *h* is hour, and *s* is seconds.

Examples

In the following example, a crashinfo file called "crashdata" will be created in the default flash memory device if a system crash occurs:

```
Router(config)# exception crashinfo file flash:crashinfo
```

Related Commands

Command	Description
exception crashinfo buffersize	Changes the size of the crashinfo buffer.

exception dump

To configure the router to dump a core file to a particular server when the router crashes, use the **exception dump** command in global configuration mode. To disable core dumps, use the **no** form of this command.

exception dump *ip-address*

no exception dump

Syntax Description

ip-address	IP address of the server that stores the core dump file.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Caution Use the **exception dump** command only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, FTP, or rcp server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

If you use TFTP to dump the core file to a server, the router will only dump the first 16 MB of the core file. If the router's memory is larger than 16 MB, the whole core file will not be copied to the server. Therefore, use rcp or FTP to dump the core file.

The core dump is written to a file named *hostname*-core on your server, where *hostname* is the name of the router. You can change the name of the core file by configuring the **exception core-file** command.

This procedure can fail for certain types of system crashes. However, if successful, the core dump file will be the size of the memory available on the processor (for example, 16 MB for a CSC/4).

Examples

In the following example, a user configures a router to use FTP to dump a core file to the FTP server at 172.17.92.2 when it crashes:

```
Router(config)# ip ftp username red
Router(config)# ip ftp password blue
Router(config)# exception protocol ftp
Router(config)# exception dump 172.17.92.2
Router(config)# exception core-file dumpfile
```

Related Commands

Command	Description
exception core-file	Specifies the name of the core dump file.
exception memory	Causes the router to create a core dump and reboot when certain memory size parameters are violated.
exception protocol	Configures the protocol used for core dumps.
exception spurious-interrupt	Causes the router to create a core dump and reload after a specified number of spurious interrupts.
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp username	Configures the username for FTP connections.
ip rcmd remote-username	Configures the remote username to be used when requesting a remote copy using rcp.

exception linecard

To enable storing of crash information for a line card and optionally specify the type and amount of information stored, use the **exception linecard** command in global configuration mode. To disable the storing of crash information for the line card, use the **no** form of this command.

exception linecard {**all** | **slot** *slot-number*} [**corefile** *filename* | **main-memory** *size* [**k** | **m**] | **queue-ram** *size* [**k** | **m**] | **rx-buffer** *size* [**k** | **m**] | **sqe-register-rx** | **sqe-register-tx** | **tx-buffer** *size* [**k** | **m**]]

no exception linecard

Syntax Description

all	Stores crash information for all line cards.
slot *slot-number*	Stores crash information for the line card in the specified slot. Slot numbers range from 0 to 11 for the Cisco 12012 and 0 to 7 for the Cisco 12008 router.
corefile *filename*	(Optional) Stores the crash information in the specified file in NVRAM. The default filename is *hostname*-**core**-*slot-number* (for example, c12012-core-8).
main-memory *size*	(Optional) Stores the crash information for the main memory on the line card and specifies the size of the crash information. Size of the memory to store is 0 to 268435456.
queue-ram *size*	(Optional) Stores the crash information for the queue RAM memory on the line card and specifies the size of the crash information. Size of the memory to store can be from 0 to 1048576.
rx-buffer *size* **tx-buffer** *size*	(Optional) Stores the crash information for the receive and transmit buffer on the line card and specifies the size of the crash information. Size of the memory to store can be from 0 to 67108864.
sqe-register-rx **sqe-register-tx**	(Optional) Stores crash information for the receive or transmit silicon queueing engine registers on the line card.
k **m**	(Optional) The **k** option multiplies the specified *size* by 1K (1024), and the **m** option multiplies the specified *size* by 1M (1024*1024).

Defaults

No crash information is stored for the line card.

If enabled with no options, the default is to store 256 MB of main memory.

Command Modes

Global configuration

Command History

Release	Modification
11.2 GS	This command was introduced for Cisco 12000 series Gigabit Switch Routers (GSRs).

Usage Guidelines

Use caution when enabling the **exception linecard** global configuration command. Enabling all options could cause a large amount (150 to 250 MB) of crash information to be sent to the server.

Caution Use the **exception linecard** global configuration command only when directed by a technical support representative. Only enable options that the technical support representative requests you to enable. Technical support representatives need to be able to look at the crash information from the line card to troubleshoot serious problems on the line card. The crash information contains all the line card memory information including the main memory and transmit and receive buffer information. .

Examples

In the following example, the user enables the storing of crash information for line card 8. By default, 256 MB of main memory is stored.

```
Router(config)# exception linecard slot 8
```

exception memory

To cause the router to create a core dump and reboot when certain memory size parameters are violated, use the **exception memory** command in global configuration mode. To disable the rebooting and core dump, use the **no** form of this command.

exception memory {**fragment** *size* | **minimum** *size*}

no exception memory {**fragment** | **minimum**}

Syntax Description

fragment *size*	The minimum contiguous block of memory in the free pool, in bytes.
minimum *size*	The minimum size of the free memory pool, in bytes.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This command is used to troubleshoot memory leaks.

The size is checked every 60 seconds. If you enter a size that is greater than the free memory, a core dump and router reload is generated after 60 seconds.

Caution Use the **exception** commands only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, FTP, or rcp server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

The **exception dump** command must be configured in order to generate a core dump file. If the **exception dump** command is not configured, the router reloads without generating a core dump.

Examples

In the following example, the user configures the router to monitor the free memory. If the amount of free memory falls below 250,000 bytes, the router will dump the core file and reload.

```
Router(config)# exception dump 131.108.92.2
Router(config)# exception core-file memory.overrun
Router(config)# exception memory minimum 250000
```

Related Commands

Command	Description
exception core-file	Specifies the name of the core dump file.
exception dump	Configures the router to dump a core file to a particular server when the router crashes.
exception protocol	Configures the protocol used for core dumps.
exception region-size	Specifies the size of the region for the exception-time memory pool.
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp username	Configures the username for FTP connections.

exception protocol

To configure the protocol used for core dumps, use the **exception protocol** command in global configuration mode. To configure the router to use the default protocol, use the **no** form of this command.

exception protocol {**ftp** | **rcp** | **tftp**}

no exception protocol

Syntax Description

ftp	Uses FTP for core dumps.
rcp	Uses rcp for core dumps.
tftp	Uses TFTP for core dumps. This is the default.

Defaults

TFTP

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Caution Use the **exception** commands only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, FTP, or rcp server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

If you use TFTP to dump the core file to a server, the router will only dump the first 16 MB of the core file. If the router's memory is larger than 16 MB, the whole core file will not be copied to the server. Therefore, use rcp or FTP to dump the core file.

Examples

In the following example, the user configures a router to use FTP to dump a core file to the FTP server at 172.17.92.2 when it crashes:

```
Router(config)# ip ftp username red
Router(config)# ip ftp password blue
Router(config)# exception protocol ftp
Router(config)# exception dump 172.17.92.2
```

Related Commands

Command	Description
exception core-file	Specifies the name of the core dump file.
exception dump	Causes the router to dump a core file to a particular server when the router crashes.
exception memory	Causes the router to create a core dump and reboot when certain memory size parameters are violated.
exception spurious-interrupt	Causes the router to create a core dump and reload after a specified number of spurious interrupts.
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp username	Configures the username for FTP connections.

exception region-size

To specify the size of the region for the exception-time memory pool, use the **exception region-size** command in global configuration mode. To use the default region size, use the **no** form of this command.

exception region-size *size*

no exception region-size

Syntax Description

size	The size of the region for the exception-time memory pool.

Defaults

16,384 bytes

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Caution Use the **exception** commands only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, FTP, or rcp server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

The **exception region-size** command is used to define a small amount of memory to serve as a fallback pool when the processor memory pool is marked corrupt. The **exception memory** command must be used to allocate memory to perform a core dump.

Examples

In the following example, the region size is set at 1024:

```
Router(config)# exception region-size 1024
```

Related Commands

Command	Description
exception core-file	Specifies the name of the core dump file.
exception dump	Configures the router to dump a core file to a particular server when the router crashes.
exception memory	Causes the router to create a core dump and reboot when certain memory size parameters are violated.
exception protocol	Configures the protocol used for core dumps.

Command	Description
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp username	Configures the username for FTP connections.

exception spurious-interrupt

To configure the router to create a core dump and reload after a specified number of spurious interrupts, use the **exception spurious-interrupt** command in global configuration mode. To disable the core dump and reload, use the **no** form of this command.

exception spurious-interrupt [*number*]

no exception spurious-interrupt

Syntax Description

number	(Optional) A number from 1 to 4294967295 that indicates the maximum number of spurious interrupts to include in the core dump before reloading.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Caution Use the **exception** commands only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, FTP, or rcp server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

If you use TFTP to dump the core dump file to a server, the router will only dump the first 16 MB of the file. If the router's memory is larger than 16 MB, the whole core file will not be copied to the server. Therefore, use rcp or FTP to dump the core file.

Examples

In the following example, the user configures a router to create a core dump with a limit of two spurious interrupts:

```
Router(config)# exception spurious-interrupt 2
```

Related Commands

Command	Description
exception core-file	Specifies the name of the core dump file.
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp username	Configures the user name for FTP connections.

exec

To allow an EXEC process on a line, use the **exec** command in line configuration mode. To turn off the EXEC process for the specified line, use the **no** form of this command.

exec

no exec

Syntax Description

This command has no arguments or keywords.

Defaults

The EXEC processes is enabled on all lines.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When you want to allow only an outgoing connection on a line, use the **no exec** command.

The **no exec** command allows you to disable the EXEC process for connections which may attempt to send unsolicited data to the router. (For example, the control port of a rack of modems attached to an auxiliary port of router.) When certain types of data are sent to a line connection, an EXEC process can start, which makes the line unavailable.

When a user tries to Telnet to a line with the EXEC process disabled, the user will get no response when attempting to log on.

Examples

The following example disables the EXEC process on line 7.

```
Router(config)# line 7
Router(config-line)# no exec
```

exec-banner

To reenable the display of EXEC and message-of-the-day (MOTD) banners on the specified line or lines, use the **exec-banner** command in line configuration mode. To suppress the banners on the specified line or lines, use the **no** form of this command.

exec-banner

no exec-banner

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled on all lines

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command determines whether the router will display the EXEC banner and the message-of-the-day (MOTD) banner when an EXEC session is created. These banners are defined with the **banner exec** and **banner motd** global configuration commands. By default, these banner are enabled on all lines. Disable the EXEC and MOTD banners using the **no exec-banner** command.

This command has no effect on the incoming banner, which is controlled by the **banner incoming** command.

The MOTD banners can also be disabled by the **no motd-banner** line configuration command, which disables MOTD banners on a line. If the **no exec-banner** command is configured on a line, the MOTD banner will be disabled regardless of whether the **motd-banner** command is enabled or disabled. Table 24 summarizes the effects of the **exec-banner** command and the **motd-banner** command.

Table 24 Banners Displayed Based On exec-banner and motd-banner Combinations

	exec-banner (default)	**no exec-banner**
motd-banner (default)	MOTD banner EXEC banner	None
no motd-banner	EXEC banner	None

For reverse Telnet connections, the EXEC banner is never displayed. Instead, the incoming banner is displayed. The MOTD banner is displayed by default, but it is disabled if either the **no exec-banner** command or **no motd-banner** command is configured. Table 25 summarizes the effects of the **exec-banner** command and the **motd-banner** command for reverse Telnet connections.

Table 25 Banners Displayed Based On exec-banner and motd-banner Combinations for Reverse Telnet Sessions to Async Lines

	exec-banner (default)	**no exec-banner**
motd-banner (default)	MOTD banner Incoming banner	Incoming banner
no motd-banner	Incoming banner	Incoming banner

Examples

The following example suppresses the EXEC and MOTD banners on virtual terminal lines 0 to 4:

```
Router(config)# line vty 0 4
Router(config-line)# no exec-banner
```

Related Commands

Command	Description
banner exec	Defines and enables a customized banner to be displayed whenever the EXEC process is initiated.
banner incoming	Defines and enables a customized message to be displayed when there is an incoming connection to a terminal line from a host on the network.
banner motd	Defines and enables a customized message-of-the-day banner.
motd-banner	Controls (enables or disables) the display of message-of-the-day banners on a specified line or lines.

exec-character-bits

To configure the character widths of EXEC and configuration command characters, use the **exec-character-bits** command in line configuration mode. To restore the default value, use the **no** form of this command.

exec-character-bits {**7** | **8**}

no exec-character-bits

Syntax Description

7	Selects the 7-bit character set. This is the default.
8	Selects the full 8-bit character set for use of international and graphical characters in banner messages, prompts, and so on.

Defaults

7-bit ASCII character set

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Setting the EXEC character width to 8 allows you to use special graphical and international characters in banners, prompts, and so on. However, setting the EXEC character width to 8 bits can cause failures. If a user on a terminal that is sending parity enters the **help** command, an "unrecognized command" message appears because the system is reading all 8 bits, and the eighth bit is not needed for the **help** command.

Note If you are using the **autoselect** function, set the activation character to the default (Return) and the value for **exec-character-bits** to 7. If you change these defaults, the application will not recognize the activation request.

Examples

The following example enables full 8-bit international character sets, except for the console, which is an ASCII terminal. It illustrates use of the **default-value exec-character-bits** global configuration command and the **exec-character-bits** line configuration command.

```
Router(config)# default-value exec-character-bits 8
Router(config)# line 0
Router(config-line)# exec-character-bits 7
```

Related Commands

Command	Description
default-value exec-character-bits	Defines the EXEC character width for either 7 bits or 8 bits.
default-value special-character-bits	Configures the flow control default value from a 7-bit width to an 8-bit width.
length	Sets the terminal screen length.
terminal exec-character-bits	Locally changes the ASCII character set used in EXEC and configuration command characters for the current session.
terminal special-character-bits	Changes the ASCII character widths to accept special characters for the current terminal line and session.

exec-timeout

To set the interval that the EXEC command interpreter waits until user input is detected, use the **exec-timeout** command in line configuration mode. To remove the timeout definition, use the **no** form of this command.

exec-timeout *minutes* [*seconds*]

no exec-timeout

Syntax Description

minutes	Integer that specifies the number of minutes. The default is 10 minutes.
seconds	(Optional) Additional time intervals in seconds.

Defaults

10 minutes

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

If no input is detected during the interval, the EXEC facility resumes the current connection. If no connections exist, the EXEC facility returns the terminal to the idle state and disconnects the incoming session.

To specify no timeout, enter the **exec-timeout 0 0** command.

Examples

The following example sets a time interval of 2 minutes, 30 seconds:

```
Router(config)# line console
Router(config-line)# exec-timeout 2 30
```

The following example sets a time interval of 10 seconds:

```
Router(config)# line console
Router(config-line)# exec-timeout 0 10
```

execute-on

To execute commands on a line card, use the **execute-on** command in privileged EXEC mode.

execute-on {**slot** *slot-number* | **all** | **master**} *command*

Syntax Description

slot *slot-number*	Executes the command on the line card in the specified slot. Slot numbers can be chosen from the following ranges: • Cisco 12012 router: 0 to 11 • Cisco 12008 access server: 0 to 7 • Cisco AS5800 access server: 0 to 13
all	Executes the command on all line cards.
master	(AS5800 only) Executes the designated command on a Dial Shelf Controller (DSC). Do not use this option; it is used for technical support troubleshooting only.
command	Cisco IOS command to remotely execute on the line card.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2 GS	This command was introduced to support Cisco 12000 series Gigabit Switch Routers.
11.3(2)AA	This command was implemented in images for the Cisco AS5800 series.

Usage Guidelines

Use this command to execute a command on one or all line cards to monitor and maintain information on one or more line cards (for example, a line card in a specified slot on a dial shelf). This allows you to issue commands remotely; that is, to issue commands without needing to log in to the line card directly. The **all** form of the command allows you to issue commands to all the line cards without having to log in to each in turn.

Though this command does not have a **no** form, note that it is possible to use the **no** form of the remotely executed commands used in this command.

Tips This command is useful when used with **show** EXEC commands (such as **show version**), because you can verify and troubleshoot the features found only on a specific line card. Please note, however, that because not all statistics are maintained on the line cards, the output from some of the **show** commands might not be consistent.

Cisco 12000 GSR Guidelines and Restrictions

You can use the **execute-on** privileged EXEC command only from Cisco IOS software running on the GRP card.

Timesaver Though you can use the **attach** privileged EXEC command to execute commands on a specific line card, using the **execute-on slot** command saves you some steps. For example, first you must use the **attach** command to connect to the Cisco IOS software running on the line card. Next you must issue the command. Finally you must disconnect from the line card to return to the Cisco IOS software running on the GRP card. With the **execute-on slot** command, you can perform three steps with one command. In addition, the **execute-on all** command allows you to perform the same command on all line cards simultaneously.

Cisco AS5800 Guidelines and Restrictions

The purpose of the command is to conveniently enable certain commands to be remotely executed on the dial shelf cards from the router without connecting to each line card. This is the recommended procedure, because it avoids the possibility of adversely affecting a good configuration of a line card in the process. The **execute-on** command does not give access to every Cisco IOS command available on the Cisco AS5800 access server. In general, the purpose of the **execute-on** command is to provide access to statistical reports from line cards without directly connecting to the dial shelf line cards.

Caution Do not use this command to change configurations on dial shelf cards, because such changes will not be reflected in the router shelf.

Using this command makes it possible to accumulate inputs for inclusion in the **show tech-support** command.

The **master** form of the command can run a designated command remotely on the router from the DSC card. However, using the console on the DSC is *not* recommended. It is used for technical support troubleshooting only.

The **show tech-support** command for each dial shelf card is bundled into the router shelf's **show tech-support** command via the **execute-on** facility.

The **execute-on** command also support interactive commands such as the following:

```
router: execute-on slave slot slot ping
```

The **execute-on** command has the same limitations and restrictions as a **vty telnet** client has; that is, it cannot reload DSC using the following command:

```
router: execute-on slave slot slot reload
```

You can use the **execute-on** command to enable remote execution of the commands included in the following partial list:

- **debug dsc clock**
- **show context**
- **show diag**
- **show environment**
- **show dsc clock**
- **show dsi**
- **show dsip**
- **show tech-support**

Examples

In the following example, the user executes the **show controllers** command on the line card in slot 4 of a Cisco 12000 series GSR:

```
Router# execute-on slot 4 show controllers

========= Line Card (Slot 4) =======

Interface POS0
Hardware is BFLC POS
lcpos_instance struct   6033A6E0
RX POS ASIC addr space  12000000
TX POS ASIC addr space  12000100
SUNI framer addr space  12000400
SUNI rsop intr status   00
CRC16 enabled, HDLC enc, int clock
no loop

Interface POS1
Hardware is BFLC POS
lcpos_instance struct   6033CEC0
RX POS ASIC addr space  12000000
TX POS ASIC addr space  12000100
SUNI framer addr space  12000600
SUNI rsop intr status   00
CRC32 enabled, HDLC enc, int clock
no loop

Interface POS2
Hardware is BFLC POS
lcpos_instance struct   6033F6A0
RX POS ASIC addr space  12000000
TX POS ASIC addr space  12000100
SUNI framer addr space  12000800
SUNI rsop intr status   00
CRC32 enabled, HDLC enc, int clock
no loop

Interface POS3
Hardware is BFLC POS
lcpos_instance struct   60341E80
RX POS ASIC addr space  12000000
TX POS ASIC addr space  12000100
SUNI framer addr space  12000A00
SUNI rsop intr status   00
CRC32 enabled, HDLC enc, ext clock
no loop
Router#
```

Related Commands

Command	Description
attach	Connects you to a specific line card for the purpose of executing commands using the Cisco IOS software image on that line card.

exit (EXEC)

To close an active terminal session by logging off the router, use the **exit** command in EXEC mode.

exit

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use the **exit** command in EXEC mode to exit the active session (log off the device). This command can be used in any EXEC mode (such as User EXEC mode or Privileged EXEC mode) to exit from the EXEC process.

Examples

In the following example, the **exit** (global) command is used to move from global configuration mode to privileged EXEC mode, the **disable** command is used to move from privileged EXEC mode to user EXEC mode, and the **exit** (EXEC) command is used to log off (exit the active session):

```
Router(config)# exit
Router# disable
Router> exit
```

Related Commands

Command	Description
disconnect	Disconnects a line.
end	Ends your configuration session by exiting to EXEC mode.
exit (global)	Exits from the current configuration mode to the next highest configuration mode.
logout	Closes your connection to the device (equivilant to the **exit** command).

exit (global)

To exit any configuration mode to the next highest mode in the CLI mode hierarchy, use the **exit** command in any configuration mode.

exit

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

All configuration modes

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **exit** command is used in the Cisco IOS CLI to exit from the current command mode to the next highest command mode in the CLI mode hierarchy.

For example, use the **exit** command in global configuration mode to return to privileged EXEC mode. Use the **exit** command in interface, line, or router configuration mode to return to global configuration mode. Use the **exit** command in subinterface configuration mode to return to interface configuration mode. At the highest level, EXEC mode, the **exit** command will exit the EXEC mode and disconnect from the router interface (see the description of the **exit** (EXEC) command for details).

Examples

The following example shows how to exit from the subinterface configuration mode and to return to the interface configuration mode:

```
Router(config-subif)# exit
Router(config-if)#
```

```
The following example displays an exit from the interface configuration mode to return to
the global configuration mode:

Router(config-if)# exit
Router(config)#
```

Related Commands

Command	Description
disconnect	Disconnects a line.
end	Ends your configuration session by exiting to privileged EXEC mode.
exit (EXEC)	Closes the active terminal session by logging off the router.

file prompt

To specify the level of prompting, use the **file prompt** command in global configuration mode.

file prompt [**alert** | **noisy** | **quiet**]

Syntax Description

alert	(Optional) Prompts only for destructive file operations. This is the default.
noisy	(Optional) Confirms all file operation parameters.
quiet	(Optional) Seldom prompts for file operations.

Defaults

alert

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Use this command to change the amount of confirmation needed for different file operations.

This command affects only prompts for confirmation of operations. The router will always prompt for missing information.

Examples

The following example configures confirmation prompting for all file operations:

```
Router(config)# file prompt noisy
```

filter-for-history

To define the type of information kept in the history table for an Service Assurance Agent (SAA) operation, use the **filter-for-history** command in SAA RTR configuration mode. To return to the default value, use the **no** form of this command.

filter-for-history {**none** | **all** | **overThreshold** | **failures**}

no filter-for-history {**none** | **all** | **overThreshold** | **failures**}

Syntax Description

none	No history kept. This is the default.
all	All operation operations attempted are kept in the history table.
overThreshold	Only packets that are over the threshold are kept in the history table.
failures	Only packets that fail for any reason are kept in the history table.

Defaults

No SAA history is kept for an operation.

Command Modes

SAA RTR configuration

SAA DHCP Configuation (config-rtr-dhcp)

SAA Echo configuration (config-rtr-echo)

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use the **filter-for-history** command to control what gets stored in the history table for the SAA. To control how much history gets saved in the history table, use the **lives-of-history-kept**, **buckets-of-history-kept**, and the **samples-of-history-kept** SAA RTR configuration commands.

An operation can collect history and capture statistics. By default, history is not collected. When a problem arises where history is useful (for example, a large number of timeouts are occurring), you can configure the **lives-of-history-kept** command to collect history.

Note Collecting history increases the RAM usage. Only collect history when you think there is a problem. For general network response time information, use statistics.

Examples

In the following example, only operation packets that fail are kept in the history table:

```
Router(config)# rtr 1
Router(config-rtr)# type echo protocol ipIcmpEcho 172.16.161.21
Router(config-rtr)# lives-of-history-kept 1
Router(config-rtr)# filter-for-history failures
```

Related Commands

Command	Description
buckets-of-history-kept	Sets the number of history buckets that are kept during the lifetime of the SAA.
lives-of-history-kept	Sets the number of lives maintained in the history table for the SAA operation.
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.
samples-of-history-kept	Sets the number of entries kept in the history table per bucket for the SAA operation.

format

To format a Class A or Class C Flash file system, use the **format** command in EXEC mode.

Class C Flash File System

format *filesystem1***:**

Class A Flash File System

format [**spare** *spare-number*] *filesystem1***:** [[*filesystem2***:**][*monlib-filename*]]

Caution Reserve a certain number of memory sectors as spares, so that if some sectors fail, most of the Flash memory card can still be used. Otherwise, you must reformat the Flash card when some of the sectors fail.

Syntax Description

spare	(Optional) Reserves spare sectors as specified by the *spare-number* argument when formatting Flash memory.
spare-number	(Optional) Number of the spare sectors to reserve on formatted Flash memory. Valid values are from 0 to 16. The default value is zero.
*filesystem1***:**	Flash memory to format, followed by a colon.
*filesystem2***:**	(Optional) File system containing the monlib file to use for formatting *filesystem1* followed by a colon.
monlib-filename	(Optional) Name of the ROM monitor library file (monlib file) to use for formatting the *filesystem1* argument. The default monlib file is the one bundled with the system software. When used with HSA and you do not specify the *monlib-filename* argument, the system takes ROM monitor library file from the slave image bundle. If you specify the *monlib-filename* argument, the system assumes that the files reside on the slave devices.

Defaults

The default monlib file is the one bundled with the system software.

The default number of spare sectors is zero (0).

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Use this command to format Class A or C Flash memory file systems.

In some cases, you might need to insert a new PCMCIA Flash memory card and load images or backup configuration files onto it. Before you can use a new Flash memory card, you must format it.

Sectors in Flash memory cards can fail. Reserve certain Flash memory sectors as "spares" by using the optional *spare* argument on the **format** command to specify 0 to 16 sectors as spares. If you reserve a small number of spare sectors for emergencies, you can still use most of the Flash memory card. If you specify 0 spare sectors and some sectors fail, you must reformat the Flash memory card, thereby erasing all existing data.

The monlib file is the ROM monitor library. The ROM monitor uses this file to access files in the Flash file system. The Cisco IOS system software contains a monlib file.

In the command syntax, *filesystem1***:** specifies the device to format and *filesystem2***:** specifies the optional device containing the monlib file used to format *filesystem1***:**. If you omit the optional *filesystem2***:** and *monlib-filename* arguments, the system formats *filesystem1***:** using the monlib file already bundled with the system software. If you omit only *the optional filesystem2***:** argument, the system formats *filesystem1***:** using the monlib file from the device you specified with the **cd** command. If you omit only the optional *monlib-filename* argument, the system formats *filesystem1***:** using the *filesystem2***:** monlib file. When you specify both arguments—*filesystem2***:** and *monlib-filename*—the system formats *filesystem1***:** using the monlib file from the specified device. You can specify *filesystem1***:**'s own monlib file in this argument. If the system cannot find a monlib file, it terminates its formatting.

Note You can read from or write to Flash memory cards formatted for Cisco 7000 series Route Processor (RP) cards in your Cisco 7200 and 7500 series routers, but you cannot boot the Cisco 7200 and 7500 series routers from a Flash memory card formatted for the Cisco 7000 series routers. Similarly, you can read from or write to Flash memory cards formatted for the Cisco 7200 and 7500 series routers in your Cisco 7000 series routers, but you cannot boot the Cisco 7000 series routers from a Flash memory card formatted for the Cisco 7200 and 7500 series routers.

Examples

The following example formats a Flash memory card inserted in slot 0:

```
Router# format slot0:

Running config file on this device, proceed? [confirm]y
All sectors will be erased, proceed? [confirm]y
Enter volume id (up to 31 characters): <Return>
Formatting sector 1 (erasing)
Format device slot0 completed
```

When the console returns to the EXEC prompt, the new Flash memory card is formatted and ready for use.

Related Commands

Command	Description
cd	Changes the default directory or file system.
copy	Copies any file from a source to a destination.
delete	Deletes a file on a Flash memory device.
show file systems	Lists available file systems.
squeeze	Permanently deletes Flash files by squeezing a Class A Flash file system.
undelete	Recovers a file marked "deleted" on a Class A or Class B Flash file system.

frequency

To set the rate at which a specified SAA operation is sent into the network, use the **frequency** command in SAA RTR configuration mode. To return to the default value, use the **no** form of this command.

frequency *seconds*

no frequency

Syntax Description

seconds	Number of seconds between the SAA probe operations.

Defaults

60 seconds

Command Modes

SAA RTR configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

If an individual SAA operational probe takes longer to execute than the specified frequency value, a statistics counter called “busy” is incremented rather than sending a second probe.

Note We recommend that you do not set the frequency value to less than 60 seconds for the following reasons: It is not needed when keeping statistics (the default), and it can slow down the WAN because of the potential overhead that numerous operations can cause.

The value specified for the **frequency** command cannot be less than the value specified for the **timeout** SAA RTR configuration command.

Examples

The following example configures SAA IP/ICMP Echo operation 1 to send a probe every 90 seconds:

```
Router(config)# rtr 1
Router(config-rtr)# type echo protocol ipIcmpEcho 172.16.1.176
Router(config-rtr)# frequency 90
```

Related Commands

Command	Description
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.
timeout	Sets the amount of time the SAA operation waits for a response from its request packet.

fsck

To check a File Allocation Table (FAT)-based disk or Class C filesystem for damage and to repair any problems, use the **fsck** command in privileged EXEC mode.

fsck [**/nocrc**] *filesystem***:** [**/automatic**]

Syntax Description

/nocrc	(Optional. This keyword is available for Class C Flash file systems only.) Omits cyclic redundancy checks (CRCs).
*filesystem***:**	The filesystem prefix indicating the disk to be checked. The colon (:) is required. Typically, the filesystem prefix will be **disk0:** or **disk1:**.
/automatic	(Optional. This keyword is available for ATA FAT-based disks only.) Specifies that the check and repair actions should proceed automatically. This option can be used to skip the prompts for each check and repair action.

Defaults

If the **/automatic** keyword is not used, CLI prompts for actions are issued.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.
12.2(13)T, 12.0(22)S	This command was implemented on the Cisco 7000 family of routers and on the Cisco 10000 and 12000 series to support ATA disks.

Usage Guidelines

This command will perform all of the steps necessary to remove corrupted files and reclaim unused disk space. Changes include checking for incorrect file sizes, cluster loops, and so on. The default form of this command will issue multiple prompts to confirm each of the changes. However, you can skip these prompts by using the **/automatic** keyword when issuing the command.

When the **/automatic** keyword is used you will prompted to confirm that you want the automatic option. Prompts for actions will be skipped, but all actions performed will be displayed to the terminal (see the example below).

This command works with ATA PCMCIA cards formatted in DOS, or for Class C Flash file systems.

Note Only one partition (the active partition) will be checked in the ATA disk.

Examples

The following example shows sample output from using the **fsck** command in automatic mode:

```
Router# fsck /automatic disk1:
Proceed with the automatic mode? [yes] y
Checking the boot sector and partition table...
Checking FAT, Files and Directories...
```

```
Start cluster of file disk1:/file1 is invalid, removing file
File disk1:/file2 has a free/bad cluster, truncating...
File disk1:/file2 truncated.
File disk1:/file3 has a free/bad cluster, truncating...
File disk1:/file3 truncated.
File disk1:/file4 has a invalid cluster, truncating...
File disk1:/file4 truncated.
File disk1:/file5 has a invalid cluster, truncating...
File disk1:/file5 truncated.
File disk1:/file6 has a invalid cluster, truncating...
File disk1:/file6 truncated.
File size of disk1:/file7 is not correct, correcting it
File disk1:/file8 cluster chain has a loop, truncating it
File disk1:/file8 truncated.
File disk1:/file9 cluster chain has a loop, truncating it
File disk1:/file9 truncated.
File disk1:/file16 has a free/bad cluster, truncating...
File disk1:/file16 truncated.
File disk1:/file20 has a free/bad cluster, truncating...
File disk1:/file20 truncated.
Reclaiming unused space...
Created file disk1:/fsck-4 for an unused cluster chain
Created file disk1:/fsck-41 for an unused cluster chain
Created file disk1:/fsck-73 for an unused cluster chain
Created file disk1:/fsck-106 for an unused cluster chain
Created file disk1:/fsck-121 for an unused cluster chain
Created file disk1:/fsck-132 for an unused cluster chain
Created file disk1:/fsck-140 for an unused cluster chain
Created file disk1:/fsck-156 for an unused cluster chain
Created file disk1:/fsck-171 for an unused cluster chain
Created file disk1:/fsck-186 for an unused cluster chain
Created file disk1:/fsck-196 for an unused cluster chain
Created file disk1:/fsck-235 for an unused cluster chain
Created file disk1:/fsck-239 for an unused cluster chain
Updating FAT...
fsck of disk1: complete
```

full-help

To get help for the full set of user-level commands, use the **full-help** command in line configuration mode.

full-help

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **full-help** command enables (or disables) an unprivileged user to see all of the help messages available. It is used with the **show ?** command.

Examples

In the following example, the **show ?** command is used first with full-help disabled. Then **full-help** is enabled for the line, and the **show ?** command is used again to demonstrate the additional help output that is displayed.

```
Router> show ?

  bootflash  Boot Flash information
  calendar   Display the hardware calendar
  clock      Display the system clock
  context    Show context information
  dialer     Dialer parameters and statistics
  history    Display the session command history
  hosts      IP domain-name, lookup style, nameservers, and host table
  isdn       ISDN information
  kerberos   Show Kerberos Values
  modemcap   Show Modem Capabilities database
  ppp        PPP parameters and statistics
  rmon       rmon statistics
  sessions   Information about Telnet connections
  snmp       snmp statistics
  terminal   Display terminal configuration parameters
  users      Display information about terminal lines
  version    System hardware and software status

Router> enable
Password:<letmein>


Router# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# line console 0
Router(config-line)# full-help
Router(config-line)# exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router# disable
Router> show ?

  access-expression  List access expression
  access-lists       List access lists
  aliases            Display alias commands
  apollo             Apollo network information
  appletalk          AppleTalk information
  arp                ARP table
  async              Information on terminal lines used as router interfaces
  bootflash          Boot Flash information
  bridge             Bridge Forwarding/Filtering Database [verbose]
  bsc                BSC interface information
  bstun              BSTUN interface information
  buffers            Buffer pool statistics
  calendar           Display the hardware calendar
 .
 .
 .
  translate          Protocol translation information
  ttycap             Terminal capability tables
  users              Display information about terminal lines
  version            System hardware and software status
  vines              VINES information
  vlans              Virtual LANs Information
  whoami             Info on current tty line
  x25                X.25 information
  xns                XNS information
  xremote            XRemote statistics
```

Related Commands

Command	Description
help	Displays a brief description of the help system.

help

To display a brief description of the help system, use the **help** command in any command mode.

help

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

User EXEC

Privileged EXEC

All configuration modes

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **help** command provides a brief description of the context-sensitive help system, which functions as follows:

- To list all commands available for a particular command mode, enter a question mark (?) at the system prompt.
- To obtain a list of commands that begin with a particular character string, enter the abbreviated command entry immediately followed by a question mark (?). This form of help is called *word help*, because it lists only the keywords or arguments that begin with the abbreviation you entered.
- To list the keywords and arguments associated with a command, enter a question mark (?) in place of a keyword or argument on the command line. This form of help is called *command syntax help*, because it lists the keywords or arguments that apply based on the command, keywords, and arguments you have already entered.

Examples

In the following example, the **help** command is used to display a brief description of the help system:

```
Router# help

Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)
```

The following example shows how to use word help to display all the privileged EXEC commands that begin with the letters “co.” The letters entered before the question mark are reprinted on the next command line to allow the user to continue entering the command.

```
Router# co?
configure  connect  copy
Router# co
```

The following example shows how to use command syntax help to display the next argument of a partially complete **access-list** command. One option is to add a wildcard mask. The <cr> symbol indicates that the other option is to press Enter to execute the command without adding any more keywords or arguments. The characters entered before the question mark are reprinted on the next command line to allow the user to continue entering the command or to execute that command as it is.

```
Router(config)# access-list 99 deny 131.108.134.234 ?
  A.B.C.D  Mask of bits to ignore
  <cr>
Router(config)# access-list 99 deny 131.108.134.234
```

Related Commands

Command	Description
full-help	Enables help for the full set of user-level commands for a line.

history

To enable the command history function, use the **history** command in line configuration mode. To disable the command history function, use the **no** form of this command.

history

no history

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled with ten command lines in the buffer.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The command history function provides a record of EXEC commands that you have entered. This function is particularly useful for recalling long or complex commands or entries, including access lists.

To change the number of command lines that the system will record in its history buffer, use the **history size** line configuration command.

The **history** command enables the history function with the last buffer size specified or, if there was not a prior setting, with the default of ten lines. The **no history** command disables the history function.

The **show history** EXEC command will list the commands you have entered, but you can also use your keyboard to display individual commands. Table 26 lists the keys you can use to recall commands from the command history buffer.

Table 26 History Keys

Key(s)	Functions
Ctrl-P or Up Arrow[1]	Recalls commands in the history buffer in a backward sequence, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Ctrl-N or Down Arrow[1]	Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow. Repeat the key sequence to recall successively more recent commands.

1. The arrow keys function only with ANSI-compatible terminals.

Examples

In the following example, the command history function is disabled on line 4:

```
Router(config)# line 4
Router(config-line)# no history
```

Related Commands

Command	Description
history size	Sets the command history buffer size for a particular line.
show history	Lists the commands you have entered in the current EXEC session.
terminal history	Enables the command history function for the current terminal session or changes the size of the command history buffer for the current terminal session.

history size

To change the command history buffer size for a particular line, use the **history size** command in line configuration mode. To reset the command history buffer size to ten lines, use the **no** form of this command.

history size *number-of-lines*

no history size

Syntax Description

number-of-lines	Specifies the number of command lines that the system will record in its history buffer. The range is from 0 to 256. The default is 10.

Defaults

10 command lines

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **history size** command should be used in conjunction with the **history** and **show history** commands. The **history** command enables or disables the command history function. The **show history** command lists the commands you have entered in the current EXEC session. The number of commands that the history buffer will show is set by the **history size** command.

Note The **history size** command only sets the size of the buffer; it does not reenable the history function. If the **no history** command is used, the **history** command must be used to reenable this function.

Examples

The following example displays line 4 configured with a history buffer size of 35 lines:

```
Router(config)# line 4
Router(config-line)# history size 35
```

Related Commands

Command	Description
history	Enables or disables the command history function.
show history	Lists the commands you have entered in the current EXEC session.
terminal history size	Enables the command history function for the current terminal session or changes the size of the command history buffer for the current terminal session.

hold-character

To define the local hold character used to pause output to the terminal screen, use the **hold-character** command in line configuration mode. To restore the default, use the **no** form of this command.

hold-character *ascii-number*

no hold-character

Syntax Description

ascii-number	ASCII decimal representation of a character or control sequence (for example, Ctrl-P).

Defaults

No hold character is defined.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The Break character is represented by zero; NULL cannot be represented. To continue the output, enter any character after the hold character. To use the hold character in normal communications, precede it with the escape character. See the "ASCII Character Set" appendix for a list of ASCII characters.

Examples

The following example sets the hold character to Ctrl-S, which is ASCII decimal character 19:

```
Router(config)# line 8
Router(config-line)# hold-character 19
```

Related Commands

Command	Description
terminal hold-character	Sets or changes the hold character for the current session.

hops-of-statistics-kept

To set the number of hops for which statistics are maintained per path for the SAA operation, use the **hops-of-statistics-kept** command in SAA RTR configuration mode. To return to the default value, use the **no** form of this command.

hops-of-statistics-kept *size*

no hops-of-statistics-kept

Syntax Description

size	Number of hops for which statistics are maintained per path. The default is 16 hops for type **pathEcho** and 1 hop for type **echo**.

Defaults

16 hops for type **pathEcho**

1 hop for type **echo**

Command Modes

SAA RTR configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

One hop is the passage of a timed packet from this router to another network device. The other network device is assumed to be a device along the path to the destination (including the destination) when the operation type is **pathEcho**, or just the destination when the type is **echo**.

When the number of hops reaches the size specified, no further hop information is stored.

Examples

The following example monitors the statistics of operation 2 for only 10 hops:

```
Router(config)# rtr 2
Router(config-rtr)# type pathecho protocol ipIcmpEcho 172.16.1.177
Router(config-rtr)# hops-of-statistics-kept 10
```

Related Commands

Command	Description
distributions-of-statistics-kept	Sets the number of statistic distributions kept per hop during the lifetime of the SAA.
hours-of-statistics-kept	Sets the number of hours for which statistics are maintained for the SAA operation.
paths-of-statistics-kept	Sets the number of paths for which statistics are maintained per hour for the SAA operation.

Command	Description
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.
statistics-distribution-interval	Sets the time interval for each statistics distribution kept for the SAA.

hostname

To specify or modify the host name for the network server, use the **hostname** command in global configuration mode.

hostname *name*

Syntax Description

name	New host name for the network server.

Defaults

The default host name is Router.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The host name is used in prompts and default configuration filenames.

Do not expect case to be preserved. Uppercase and lowercase characters look the same to many internet software applications. It may seem appropriate to capitalize a name the same way you might do in English, but conventions dictate that computer names appear all lowercase. For more information, refer to RFC 1178, *Choosing a Name for Your Computer.*

The name must also follow the rules for ARPANET host names. They must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. Names must be 63 characters or fewer. A host name of less than 10 characters is recommended. For more information, refer to RFC 1035, *Domain Names—Implementation and Specification*.

On most systems, a field of 30 characters is used for the host name and the prompt in the CLI. Note that the length of your host name may cause longer configuration mode prompts to be truncated. For example, the full prompt for service profile configuration mode is:

```
(config-service-profile)#
```

However, if you are using the host-name of "Router", you will only see the following prompt (on most systems):

```
Router(config-service-profil)#
```

If the hostname is longer, you will see even less of the prompt:

```
Basement-rtr2(config-service)#
```

Keep this behavior in mind when assigning a name to your system (using the **hostname** global configuration command). If you expect that users will be relying on mode prompts as a CLI navigation aid, you should assign host names of no more than nine characters.

Examples

The following example changes the host name to “sandbox”:

```
Router(config)# hostname sandbox
sandbox(config)#
```

Related Commands

Command	Description
setup	Enables you to make major changes to your configurations, for example, adding a protocol suit, making major addressing scheme changes, or configuring newly installed interfaces.

hours-of-statistics-kept

To set the number of hours for which statistics are maintained for the Service Assurance Agent (SAA) operation, use the **hours-of-statistics-kept** command in SAA RTR configuration mode. To return to the default value, use the **no** form of this command.

hours-of-statistics-kept *hours*

no hours-of-statistics-kept

Syntax Description

hours	Number of hours that the router maintains statistics. The default is 2 hours.

Defaults

2 hours

Command Modes

SAA RTR configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

When the number of hours exceeds the specified value, the statistics table wraps (that is, the oldest information is replaced by newer information).

This command sets the amount of time statistics are kept for use by the **show rtr collection-statistics** command and **show rtr distribution** command.

Examples

The following example maintains 3 hours of statistics for SAA operation 2:

```
Router(config)# rtr 2
Router(config-rtr)# type pathecho protocol ipIcmpEcho 172.16.1.177
Router(config-rtr)# hours-of-statistics-kept 3
```

Related Commands

Command	Description
distributions-of-statistics-kept	Sets the number of statistic distributions kept per hop during the lifetime of the SAA.
hops-of-statistics-kept	Sets the number of hops for which statistics are maintained per path for the SAA operation.
paths-of-statistics-kept	Sets the number of paths for which statistics are maintained per hour for the SAA operation.
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.
statistics-distribution-interval	Sets the time interval for each statistic distribution kept for the SA Agent.

http-raw-request

To explicitly specify the options for a GET request for an Service Assurance Agent (SAA) HTTP operation, use the **http-raw-request** command in SAA RTR configuration mode.

http-raw-request

Syntax Description

This command has no arguments or keywords.

Defaults

No options are specified for a GET request.

Command Modes

SAA RTR configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Using the **http-raw-request** command puts the CLI in HTTP Raw Request configuration mode, indicated by the (config-rtr-http) router prompt.

The **http-raw-request** command should follow the **type http operation raw** command. Use the raw-request command when you wish to explicitly specify the content of an HTTP request. Use HTTP 1.0 commands in HTTP Raw Request configuration mode.

The SAA will specify the content of an HTTP request for you if you use the **type http operation get** command. The SAA will send the HTTP request, receive the reply, and report Round-trip Time (RTT) statistics (including the size of the page returned).

Examples

In the following example, SAA operation 6 is created and configured as an HTTP operation. The HTTP **GET** command is explicitly specified:

```
Router(config)# rtr 6
Router(config-rtr)# type http operation raw url http://www.cisco.com
Router(config-rtr)# http-raw-request
Router(config-rtr-http)# GET /index.html HTTP/1.0\r\n
Router(config-rtr-http)# \r\n
Router(config-rtr-http)# exit
Router(config)# rtr schedule 6 start-time now
```

Related Commands

Command	Description
type http	Configures an HTTP SAA operation.

insecure

To configure a line as insecure, use the **insecure** command in line configuration mode. To disable this function, use the **no** form of this command.

insecure

no insecure

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command to identify a modem line as insecure for DEC local area transport (LAT) classification.

Examples

In the following example, line 10 is configured as an insecure dialup line:

```
Router(config)# line 10
Router(config-line)# insecure
```

international

If you are using Telnet to access a Cisco IOS platform and you want to display 8-bit and multibyte international characters (for example, Kanji) and print the Escape character as a single character instead of as the caret and bracket symbols (^[), use the **international** command in line configuration mode. To display characters in 7-bit format, use the **no** form of this command.

international

no international

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Line configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

If you are configuring a Cisco IOS platform using the Cisco web browser user interface (UI), this function is enabled automatically when you enable the Cisco web browser UI using the **ip http server** global configuration command.

Examples

The following example enables a Cisco IOS platform to display 8-bit and multibyte characters and print the Escape character as a single character instead of as the caret and bracket symbols (^[) when you are using Telnet to access the platform:

```
line vty 4
 international
```

Related Commands

Command	Description
terminal international	Prints the Escape character as a single character instead of as the caret and bracket symbols (^[) for a current Telnet session in instances when you are using Telnet to access a Cisco IOS platform and you want to display 8-bit and multibyte international characters (for example, Kanji).

ip bootp server

To enable the Bootstrap Protocol (BOOTP) service on your routing device, use the **ip bootp server** command in global configuration mode. To disable BOOTP services, use the **no** form of the command.

ip bootp server

no ip bootp server

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

By default, the BOOTP service is enabled. When disabled, the **no ip bootp server** command will appear in the configuration file.

The integrated Dynamic Host Configuration Protocol (DHCP) server was introduced in Cisco IOS Release 12.0(1)T. Because DHCP is based on BOOTP, both of these services share the “well-known” UDP server port of 67 (per RFC 951, RFC 1534, and RFC 2131). If both the BOOTP server and DHCP server are disabled, ‘ICMP port unreachable’ messages will be sent in response to incoming requests on port 67, and the original incoming packet will be discarded.

Note As with all minor services, the async line BOOTP service should be disabled on your system if you do not have a need for it in your network.

Any network device that has User Data Protocol (UDP), TCP, BOOTP, DHCP or Finger services should be protected by a firewall or have the services disabled to protect against Denial of Service attacks.

Examples

In the following example, BOOTP services are disabled on the router:

```
Router(config)# no ip bootp server
```

ip director cache refresh

To enable the DistributedDirector Cache Auto Refresh function, use the **ip director cache refresh** command in global configuration mode. To disable automatic background refresh, use the **no** form of this command.

ip director cache refresh

no ip director cache refresh

Syntax Description

This command has no keywords or arguments.

Defaults

Automatic background refresh is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

The sorting cache on DistributedDirector must be enabled before you can use the **ip director cache refresh** command. To enable the sorting cache, use the **ip director cache** command.

Once automatic background refresh for the DistributedDirector cache is enabled, the cache will actively and continuously update every expired entry by processing a fake Domain Name System (DNS) request. The cache accumulates and updates answers to all past DNS queries received since cache auto refresh was initiated. Any repeat DNS request is always serviced directly from the cache.

Examples

The following example enables automatic background refresh for the DistributedDirector cache:

```
Router(config)# ip director cache
Router(config)# ip director cache refresh

Router# show running-config

ip host myhost 172.2.2.10 172.2.2.20 172.2.2.30
.
.
.
ip director cache refresh
```

ip director cache size

To configure the variable size of the DistributedDirector cache, use the **ip director cache size** command in global configuration mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

ip director cache size *entries*

no ip director cache size *entries*

Syntax Description

entries	Maximum number of cache entries. Range is from 1 to 4294967295.

Defaults

Maximum number of cache entries: 2000

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Use the **ip director cache size** command to configure the maximum number of cache entries that the DistributedDirector system will retain in its cache. This cache size is the maximum number of cache entries that are displayed when the user enters the **show ip director cache** command.

Examples

The following example configures the maximum number of cache entries:

```
Router(config)# ip director cache size 1500
Cache size shrinked to 1500

Router# show ip director cache
Director cache is on
Cache current size = 0 maximum size = 1500
Cache time for sort cache entries: 60 secs
Director sort cache hits = 0
```

Related Commands

Command	Description
ip director cache	Enables the sorting cache on DistributedDirector.
ip director cache time	Configures how long the DistributedDirector system will retain per-client sorting information.

ip director cache time

To configure how long the DistributedDirector system will retain per-client sorting information, use the **ip director cache time** command in global configuration mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

ip director cache time *seconds*

no ip director cache time *seconds*

Syntax Description

seconds	Amount of time the per-client sorting information is retained, in number of seconds. Range is from 1 to 2147483. The default is 60 seconds.

Defaults

60 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Use the **ip director cache time** command to specify how long the DistributedDirector system will retain per-client sorting in its cache. This cache time is the maximum amount of cache time displayed when the user enters the **show ip director cache** command.

Examples

The following example configures how long the DistributedDirector system will retain per-client sorting information:

```
Router(config)# ip director cache time 100

Router# show ip director cache
Director cache is on
Cache current size = 0 maximum size = 2000
Cache time for sort cache entries: 100 secs
Director sort cache hits = 0
```

Related Commands

Command	Description
ip director cache	Enables the sorting cache on DistributedDirector.
ip director cache size	Configures the variable size of the DistributedDirector cache.

ip director default priorities

To set a default priority for a specific metric on the DistributedDirector, use the **ip director default priorities** command in global configuration mode. To remove a default priority for a metric, use the **no** form of this command.

ip director default priorities [**drp-int** *number*] [**drp-ext** *number*] [**drp-ser** *number*] [**random** *number*] [**admin** *number*] [**drp-rtt** *number*] [**portion** *number*] [**availability** *number*] [**route-map** *number*] [**boomerang** *number*]

no ip director default priorities [**drp-int** *number*] [**drp-ext** *number*] [**drp-ser** *number*] [**random** *number*] [**admin** *number*] [**drp-rtt** *number*] [**portion** *number*] [**availability** *number*] [**route-map** *number*] [**boomerang** *number*]

Syntax Description

drp-int	(Optional) DRP internal metric.
number	Numeric value of a priority level for a given metric. Range is from 1 to 100.
drp-ext	(Optional) DRP external metric.
drp-ser	(Optional) DRP server metric.
random	(Optional) Random metric.
admin	(Optional) Administrative metric.
drp-rtt	(Optional) DRP round-trip time metric.
portion	(Optional) Portion metric.
availability	(Optional) Availability metric.
route-map	(Optional) Route-map metric.
boomerang	(Optional) Boomerang metric.

Defaults

No default priorities are specified.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(8)T	The boomerang metric was added.

Usage Guidelines

Not all of the metrics need to be specified, but at least one must be specified. If the boomerang metric is specified for a given host name, then all metrics of lower priority (that is, having a higher priority number) than boomerang are always ignored.

The default priorities specified will take effect if no priorities are specified in the **ip director host priority** command or in the corresponding Domain Name System (DNS) text record for the host.

To set the default priority for several metrics, enter the metric keywords and values to be configured on the same line as the **ip director default priorities** command.

Examples

In the following example, the boomerang metric is selected as the default priority:

```
Router(config)# ip director default priorities boomerang 1

Router# show running-config

ip host boom1 172.2.2.10 172.2.2.20 172.2.2.30
ip director server 172.2.2.20 drp-association 172.4.4.2
ip director server 172.2.2.30 drp-association 172.4.4.3
ip director server 172.2.2.10 drp-association 172.4.4.1
ip director host boom1
no ip director cache
ip dns primary boom1 soa boom1 boom1@com
ip director host boom1 priority boomerang 1
no ip director drp synchronized
```

Related Commands

Command	Description
ip director access-list	Defines an access list for DistributedDirector that specifies which subdomain names and host names should be sorted.
ip director cache	Enables the sorting cache on DistributedDirector.
ip director default priorities	Sets a default priority for a specific metric on DistributedDirector.
ip director default weights	Configures default weight metrics for DistributedDirector.
ip director host priority	Configures the order in which DistributedDirector considers metrics when picking a server.
ip director host weights	Sets host-specific weights for the metrics that DistributedDirector uses to determine the best server within a specific host name.
ip director server admin-pref	Configures a per-service administrative preference value.
ip director server portion	Sets the portion value for a specific server.
ip director server preference	Specifies DistributedDirector preference of one server over others or takes a server out of service.
show ip director default priority	Verifies the default configurations of DistributedDirector metrics.
show ip director default weights	Shows DistributedDirector default weights.
show ip director servers	Displays DistributedDirector server preference information.

ip director default weights

To configure default weight metrics for DistributedDirector, use the **ip director default weights** command in global configuration mode. To set the defaults to zero, use the **no** form of this command.

ip director default weights {[**drp-int** *number*] [**drp-ext** *number*] [**drp-ser** *number*] [**drp-rtt** *number*] [**random** *number*] [**admin** *number*] [**portion** *number*] [**availability** *number*] [**route-map** *number*]}

no ip director default weights {[**drp-int** *number*] [**drp-ext** *number*] [**drp-ser** *number*] [**drp-rtt** *number*] [**random** *number*] [**admin** *number*] [**portion** *number*] [**availability** *number*] [**route-map** *number*]}

Syntax Description

drp-int *number*	(Optional) Director Response Protocol (DRP) internal metric. The range is 1 to 100. This option sends a DRP request to all DRP server agents, asking them for the distance from themselves to the edge of their Border Gateway Protocol (BGP) autonomous system in the direction of the client originating the Domain Name System (DNS) query. This distance can be used along with the DRP external metric (**drp-ext**) to help determine the distance between the router and the client originating the DNS query. If the client and the DRP server agent are in the same autonomous system, this metric returns the Interior Gateway Protocol (IGP) cost metric between the client and the DRP server agent.
drp-ext *number*	(Optional) DRP external metric. The range is 1 to 100. This option sends a DRP request to all DRP server agents, asking them for the BGP distance between them and the client originating the DNS query. This distance represents the number of BGP hops between the autonomous system of the DRP server agent and the autonomous system of the client originating the DNS query. Because this is BGP information, the DRP server agents need to have access to full Internet BGP information in order for this metric to be useful.
drp-ser *number*	(Optional) DRP server metric. The range is 1 to 100. This option sends a DRP request to all DRP server agents, asking them for the IGP route metric between them and the distributed servers that they support. This distance can be used with the DRP internal metric (**drp-int**) to get a finer distance calculation between the distributed servers and the edge of the BGP autonomous system in the direction of the client originating the DistributedDirector query. If a true BGP border router is used as a DRP server agent, the DRP server metric will return the IGP route metric between the distributed server and the BGP border router (autonomous system edge). Because DRP server metrics should not change frequently, DistributedDirector issues DRP server queries (and caches the results) every 10 minutes.
drp-rtt *number*	(Optional) DRP round-trip time metric. The range is 1 to 100. This option sends a DRP request to all DRP server agents, asking them for the round-trip time between the DRP agent and the client originating the DNS query.

random *number*	(Optional) Random metric. The range is 1 to 100. This option selects a random number for each distributed server and defines the "best" server as the one with the smallest random number assignment. Using this metric alone results in random redirection of clients to the distributed servers. Because this metric requires no routing table information, it does not trigger DRP requests to the DRP server agents.
admin *number*	(Optional) Administrative metric. The range is 1 to 100. This option specifies a simple preference of one server over another. If the administrative metric has been explicitly set to zero, the Director will not consider the server, so the server is taken out of service.
portion *number*	(Optional) Portion metric. The range is 1 to 100. This option assigns a load "portion" to each server such that servers with a higher portion value will receive a larger percentage of connections at any one time.
availability *number*	(Optional) Availability metric. The range is 1 to 65535. This option specifies the load information for the DistributedDirector. The default value is 65,535.
route-map *number*	(Optional) Route-map metric. The range is 1 to 100. This option specifies if a server should be offered to a client.

Defaults

No default weights are specified.

The availability default value is 65535.

Command Modes

Global configuration

Command History

Release	Modification
11.1(18)IA	This command was introduced.
12.1(5)T	The availability and route-map metrics were added.
12.2(4)T3	The command name was changed slightly: **default weights** replaced **default-weights**.

Usage Guidelines

Not all the metrics need to be configured; however, at least one metric must be configured when this command is used.

Default weights are used for all host names sorted by the DistributedDirector. To override default weights for a certain host, specify host-specific weights in the private DNS server configuration.

When the associated metric is referenced in the sorting decision, it will always be multiplied by the appropriate metric weight. In this way, you can specify that some metrics be weighted more than others. You may determine the weights that you want to use through experimentation. The weights given do not need to add up to 100.

The new availability metric allows the DistributedDirector to attempt to create a TCP connection to each distributed server on a configured port over a configurable time interval.

Examples

The following command configures default weights for the internal and external metrics:

```
Router(config)# ip director default weight drp-int 10 drp-ext 90
```

Related Commands

Command	Description
debug ip director parse	Shows debugging information for DistributedDirector parsing of TXT information.
debug ip director sort	Shows debugging information for DistributedDirector IP address sorting.
ip director access-list	Defines an access list for the DistributedDirector that specifies which subdomain names and host names should be sorted.
ip director cache	Enables the sorting cache on the DistributedDirector.
ip director default priorities	Sets default priorities for a specific metric on the DistributedDirector.
ip director drp rttprobe	Sets the protocol used by DRP agents for RTT probing in DistributedDirector.
ip director host priority	Configures the order in which the DistributedDirector considers metrics when selecting a server.
ip director host weights	Sets host-specific weights for the metrics that the DistributedDirector uses to determine the best server within a specific host name.
ip director server admin-pref	Configures a per-service administrative preference value.
ip director server portion	Sets the portion value for a specific server.
ip director server preference	Specifies DistributedDirector preference of one server over others or takes a server out of service.
show ip director default priority	Verifies the default configurations of DistributedDirector metrics.
show ip director default weights	Shows the DistributedDirector default weights.
show ip director servers	Displays the DistributedDirector server preference information.

ip director dfp security

To configure a security key for use when connecting to the Dynamic Feedback Protocol (DFP) client named, use the **ip director dfp security** command in global configuration mode. To turn off the security key, use the **no** form of this command.

ip director dfp security *ip-address* **md5** *string* [*timeout*]

no ip director dfp security *ip-address* **md5** *string* [*timeout*]

Syntax Description

ip-address	IP address for the service.
md5	Security data authentication. Message Digest 5.
string	Security key.
timeout	(Optional) Amount of time, in seconds, during which DistributedDirector will continue to accept a previously defined security key. The default value is 0 seconds.

Defaults

The timeout default value is 0 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

The **ip director dfp security** command should be entered before configuring the **ip director dfp** command, resulting in a connection being made, but it can be entered independently of making a connection.

DFP allows servers to take themselves Out-of-Service and place themselves back In-Service. This function could result in a security risk because a network that is hacked could be shut down even though all the servers are still performing. An optional security vector is included in DFP to allow each message to be verified. The security vector is used to describe the security algorithm being used and to provide the data for that algorithm. The security vector itself is also extensible in that it specifies which security algorithm is being used. This specification allows different levels of security from MD5 to Data Encryption Standard (DES) to be used without overhauling the protocol and disrupting any installed base of equipment. If a receiving unit is configured for the specified security type, all DFP packets must contain that security vector or they are ignored. If a receiving unit is not configured for any security type, the security vector does not have to be present, and if it is present, it is ignored while the rest of the message is processed normally.

Examples

The following example configures the security key hello:

```
ip director dfp security 10.0.0.1 md5 hello 60
```

Related Commands

Command	Purpose
ip director dfp	Configures the DistributedDirector DFP agent with which the DistributedDirector should communicate.

ip director dfp

To configure the DistributedDirector Dynamic Feedback Protocol (DFP) agent with which the DistributedDirector should communicate, use the **ip director dfp** command in global configuration mode. To turn off the DFP agent, use the **no** form of this command.

ip director dfp *ip-address* [*port*] [**retry** *number*] [**attempts** *seconds*] [**timeout** *seconds*]

no ip director dfp *ip-address* [*port*] [**retry** *number*] [**attempts** *seconds*] [**timeout** *seconds*]

Syntax Description

ip-address	IP address.
port	(Optional) Port number to which the distributed servers are configured. The default value is 8080.
retry *number*	(Optional) Number of times a connection will be attempted. The default value is 5 attempts.
attempts *seconds*	(Optional) Delay, in seconds, between each attempt. The default value is 10,000 seconds.
timeout *seconds*	(Optional) Maximum amount of time, in seconds, for which DFP information is assumed valid. The default value is 10,000 seconds.

Defaults

The port default value is 8080.

The retry default value is 5 attempts.

The attempts default value is 10000 seconds.

The timeout default value is 10000 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

A connection is attempted a specified number of times with a delay of a specified number of seconds between each attempt. Once a connection is established, the DFP protocol will run. If a time interval update has not occurred for this DFP session, the connection breaks and is reestablished as described above.

Examples

The following example configures the DistributedDirector to communicate with a specified DFP agent:

```
ip director dfp 10.0.0.1 retry 3 attempts 60 timeout 6000
```

ip director drp rttprobe

To set the protocol used by Director Response Protocol (DRP) agents for round-trip time (RTT) probing in DistributedDirector, use the **ip director drp rttprobe** command in global configuration mode. To disable the use of a protocol, use the **no** form of the command.

ip director drp rttprobe [**tcp** | **icmp**]

no ip director drp rttprobe [**tcp** | **icmp**]

Syntax Description

tcp	(Optional) Transmission Control Protocol. This is the default.
icmp	(Optional) Internet Control Message Protocol.

Defaults

TCP

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

Both protocols can be activated, in which case DistributedDirector will instruct DRP agents to return the RTT collected from either the TCP or Internet Control Message Protocol (ICMP) protocol, whichever becomes available first. At any time, at least one of the protocols must be active.

To use only one protocol, enable the protocol you want to use, and then disable the protocol that was already configured.

```
Router(config)# ip director drp rttprobe icmp
Router(config)# no ip director drp rttprobe tcp
```

Examples

The following example shows that ICMP is configured for use by DRP agents for RTT probing:

```
Router(config)# ip director drp rttprobe icmp
```

Related Commands

Command	Description
ip director access-list	Defines an access list for the DistributedDirector that specifies which subdomain names and host names should be sorted.
ip director cache	Enables the sorting cache on the DistributedDirector.
ip director default priorities	Sets default priorities for a specific metric on the DistributedDirector.
ip director default weights	Configures default weight metrics for the DistributedDirector.

Command	Description
ip director host priority	Configures the order in which the DistributedDirector considers metrics when selecting a server.
ip director host weights	Sets host-specific weights for the metrics that the DistributedDirector uses to determine the best server within a specific host name.
ip director server admin-pref	Configures a per-service administrative preference value.
ip director server portion	Sets the portion value for a specific server.
ip director server preference	Specifies DistributedDirector preference of one server over others or takes a server out of service.
show ip director default priority	Verifies the default configurations of DistributedDirector metrics.
show ip director default weights	Shows the DistributedDirector default weights.
show ip director servers	Displays the DistributedDirector server preference information.

ip director drp synchronized

To activate clock synchronization between DistributedDirector and Director Response Protocol (DRP), use the **ip director drp synchronized** command in global configuration mode. To deactivate synchronization between the clocks in DistributedDirector and the DRPs, use the **no** form of this command.

ip director drp synchronized

no ip director drp synchronized

Syntax Description

This command has no arguments or keywords.

Defaults

Clock synchronization is deactivated.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

This command is used in conjunction with boomerang racing.

When the **ip dir drp synchronized** command is configured, DistributedDirector specifies an absolute time at which the DRP agent should respond to the DNS client.

When **no ip director drp synchronized** is configured (which is the default), DistributedDirector specifies a relative time (based on the delay measured between DistributedDirector and the DRP agent) at which the DRP agent should respond to the Domain Name Service (DNS) client.

Examples

In the following example, DistributedDirector and DRP clock synchronization are activated:

```
Router(config)# ip director drp synchronized

Router(config)# show running-config

ip host boom1 172.2.2.10 172.2.2.20 172.2.2.30
ip director server 172.2.2.20 drp-association 172.4.4.2
ip director server 172.2.2.30 drp-association 172.4.4.3
ip director server 172.2.2.10 drp-association 172.4.4.1
ip director host boom1
.
.
.
ip director drp synchronized
```

ip director host priority

To configure the order in which the DistributedDirector considers metrics when picking a server, use the **ip director host priority** command in global configuration mode. To turn off metric priorities, use the **no** form of this command.

ip director host *host-name* **priority** {[**drp-int** *number*] [**drp-ext** *number*] [**drp-ser** *number*] [**drp-rtt** *number*] [**random** *number*] [**admin** *number*] [**portion** *number*] [**availability** *number*] [**route-map** *number*]}

no ip director host *host-name* **priority** {[**drp-int** *number*] [**drp-ext** *number*] [**drp-ser** *number*] [**drp-rtt** *number*] [**random** *number*] [**admin** *number*] [**portion** *number*] [**availability** *number*] [**route-map** *number*]}

Syntax Description

host-name	Name of the host that maps to one or more IP addresses. Use the *host-name* argument to name the host that maps to one or more IP addresses. Do not use an IP address.
drp-int *number*	(Optional) Director Response Protocol (DRP) internal metric. The range is 1 to 100. This option sends a DRP request to all DRP server agents, asking them for the distance from themselves to the edge of their Border Gateway Protocol (BGP) autonomous system in the direction of the client originating the Domain Name System (DNS) query. This distance can be used along with the DRP external metric (**drp-ext**) to help determine the distance between the router and the client originating the DNS query. If the client and the DRP server agent are in the same autonomous system, this metric returns the Interior Gateway Protocol (IGP) cost metric between the client and the DRP server agent.
drp-ext *number*	(Optional) DRP external metric. The range is 1 to 100. This option sends a DRP request to all DRP server agents, asking them for the BGP distance between them and the client originating the DNS query. This distance represents the number of BGP hops between the autonomous system of the DRP server agent and the autonomous system of the client originating the DNS query. Because this is BGP information, the DRP server agents need to have access to full Internet BGP information in order for this metric to be useful.
drp-ser *number*	(Optional) DRP server metric. The range is 1 to 100. This option sends a DRP request to all DRP server agents, asking them for the IGP route metric between them and the distributed servers that they support. This distance can be used with the DRP internal metric (**drp-int**) to get a finer distance calculation between the distributed servers and the edge of the BGP autonomous system in the direction of the client originating the DistributedDirector query. If a true BGP border router is used as a DRP server agent, the DRP server metric will return the IGP route metric between the distributed server and the BGP border router (autonomous system edge). Because DRP server metrics should not change frequently, DistributedDirector issues DRP server queries (and caches the results) every 10 minutes.

drp-rtt *number*	(Optional) DRP round-trip time metric. The range is 1 to 100. This option sends a DRP request to all DRP server agents, asking them for the round-trip time between the DRP agent and the client originating the DNS query.
random *number*	(Optional) Random metric. The range is 1 to 100. This option selects a random number for each distributed server and defines the "best" server as the one with the smallest random number assignment. Using this metric alone results in random redirection of clients to the distributed servers. Because this metric requires no routing table information, it does not trigger DRP requests to the DRP server agents.
admin *number*	(Optional) Administrative metric. The range is 1 to 100. This option specifies a simple preference of one server over another. If the administrative metric has been explicitly set to zero, the Director will not consider the server, so the server is taken out of service.
portion *number*	(Optional) Portion metric. The range is 1 to 100. This option assigns a load "portion" to each server such that servers with a higher portion value will receive a larger percentage of connections at any one time.
availability *number*	(Optional) Availability metric. The range is 1 to 65,535. This option specifies the load information for the DistributedDirector. The default value is 65,535.
route-map *number*	(Optional) Route-map metric. The range is 1 to 100. This option specifies if a server should be offered to a client.

Defaults

The availability default value is 65,535.

Command Modes

Global configuration

Command History

Release	Modification
11.1(18)IA	This command was introduced.
12.1(5)T	This command was integrated into 12.1 T. The **availability** and **route-map** metrics were added.
12.2(8)T	The **boomerang** metric was added.

Usage Guidelines

Not all of the metrics need to be specified, but at least one must be specified. If the boomerang metric is specified at a given priority level, then all other metrics of lower priority (that is, having a higher priority number) for that host name are ignored. If the boomerang metric is being considered, then it is the final step in determining the best server.

The **availability** keyword allows the DistributedDirector to attempt to create a TCP connection to each distributed server on a configured port over a configurable time interval.

If multiple servers end up with the same metric value, the next metric is considered to determine the "best" server. If multiple metrics have the same priority value, the metrics are added to obtain a *composite metric*. For example, if two metrics have the same priority value, they are first multiplied by their weight values (if specified) and then added together to form the composite metric.

If you do not specify weights for a group of distributed servers, there are no default weights for the Director, and if you have specified priority values, the weight values are set to 1.

Any metrics that have a nonzero weight and that are assigned no priority value are set to a priority value of 101. They are considered after all other metrics that have priority values. As a result, if no priority values are specified for any metric, metrics are treated additively to form one composite metric.

If you do not use priority and multiple servers have the same metric value, the server whose last IP address was looked at will be returned as the "best" server. If you want to return a random IP address in the case of a tie, use metric priority with the **random** metric as the last criterion.

To turn off all priorities on all metrics associated with the defined host name, use the **no ip director host priority** command. You can turn off the priority for a specific metric or metrics using the **no ip director host** *host-name* **priority** [**drp-int** *number*] [**drp-ext** *number*] [**drp-ser** *number*] [**drp-rtt** *number*] [**random** *number*] [**admin** *number*] [**portion** *number*] [**availability** *number*] [**route-map** *number*] command.

Examples

The following example sets the external metric as the first priority and the administrative metric as the second priority:

```
Router(config)# ip director host www.xyz.com priority drp-ext 1 admin 2
```

The following example specifies the per-host priority of the metric, with a host named boom1, where the DRP internal metric is specified with a priority number of 1 and boomerang is specified with a priority number of 2:

```
Router(config)# ip director host BOOM1 priority drp-int 1 boomerang 2

Router(config)# do show running-config

ip host BOOM1 172.2.2.10 172.2.2.20 172.2.2.30
.
.
.
ip director host BOOM1
no ip director cache
ip dns primary boom1 soa boom1 boom1@com
ip director host boom1 priority drp-int 1 boomerang 2
```

Related Commands

Command	Description
ip director default priorities	Sets a default priority for a specific metric on DistributedDirector.
ip director default weights	Configures default weight metrics for DistributedDirector.
ip director host connect	Enables the DistributedDirector to verify that a server is available.
ip director host weights	Sets host-specific weights for the metrics that DistributedDirector uses to determine the best server within a specific host name.
show ip director default priority	Verifies the default configurations of DistributedDirector metrics.

Command	Description
show ip director default weights	Shows DistributedDirector default weights.
show ip director hosts	Displays DistributedDirector host information.

ip director host weights

To set host-specific weights for the metrics that the DistributedDirector uses to determine the best server within a specific host name, use the **ip director host weights** command in global configuration mode. To turn off weights for a host, use the **no** form of this command.

ip director host *host-name* **weights** {[**drp-int** *number*] [**drp-ext** *number*] [**drp-ser** *number*] [**drp-rtt** *number*] [**random** *number*] [**admin** *number*] [**portion** *number*] [**availability** *number*] [**route-map** *number*]}

no ip director host *host-name* **weights** {[**drp-int** *number*] [**drp-ext** *number*] [**drp-ser** *number*] [**drp-rtt** *number*] [**random** *number*] [**admin** *number*] [**portion** *number*] [**availability** *number*] [**route-map** *number*]}

Syntax Description

host-name	Name of the host that maps to one or more IP addresses. Do not use an IP address.
drp-int *number*	(Optional) Director Response Protocol (DRP) internal metric. The range is 1 to 100. This option sends a DRP request to all DRP server agents, asking them for the distance from themselves to the edge of their Border Gateway Protocol (BGP) autonomous system in the direction of the client originating the Domain Name System (DNS) query. This distance can be used along with the DRP external metric (**drp-ext**) to help determine the distance between the router and the client originating the DNS query. If the client and the DRP server agent are in the same autonomous system, this metric returns the Interior Gateway Protocol (IGP) cost metric between the client and the DRP server agent.
drp-ext *number*	(Optional) DRP external metric. The range is 1 to 100. This option sends a DRP request to all DRP server agents, asking them for the BGP distance between them and the client originating the DNS query. This distance represents the number of BGP hops between the autonomous system of the DRP server agent and the autonomous system of the client originating the DNS query. Because this is BGP information, the DRP server agents need to have access to full Internet BGP information in order for this metric to be useful.
drp-ser *number*	(Optional) DRP server metric. The range is 1 to 100. This option sends a DRP request to all DRP server agents, asking them for the IGP route metric between them and the distributed servers that they support. This distance can be used with the DRP internal metric (**drp-int**) to get a finer distance calculation between the distributed servers and the edge of the BGP autonomous system in the direction of the client originating the DistributedDirector query. If a true BGP border router is used as a DRP server agent, the DRP server metric will return the IGP route metric between the distributed server and the BGP border router (autonomous system edge). Because DRP server metrics should not change frequently, DistributedDirector issues DRP server queries (and caches the results) every 10 minutes.

drp-rtt *number*	(Optional) DRP round-trip time metric. The range is 1 to 100. This option sends a DRP request to all DRP server agents, asking them for the round-trip time between the DRP agent and the client originating the DNS query.
random *number*	(Optional) Random metric. The range is 1 to 100. This option selects a random number for each distributed server and defines the "best" server as the one with the smallest random number assignment. Using this metric alone results in random redirection of clients to the distributed servers. Because this metric requires no routing table information, it does not trigger DRP requests to the DRP server agents.
admin *number*	(Optional) Administrative metric. The range is 1 to 100. This option specifies a simple preference of one server over another. If the administrative metric has been explicitly set to zero, the Director will not consider the server, so the server is taken out of service.
portion *number*	(Optional) Portion metric. The range is 1 to 100. This option assigns a load "portion" to each server such that servers with a higher portion value will receive a larger percentage of connections at any one time.
availability *number*	(Optional) Availability metric. The range is 1 to 65,535. This option specifies the load information for the DistributedDirector. The default value is 65,535.
route-map *number*	(Optional) Route-map metric. The range is 1 to 100. This option specifies if a server should be offered to a client.

Note No host weights are set. If the **ip director default-weights** command is configured, the configured weights are the default.

Defaults

The availability default value is 65,535.

Command Modes

Global configuration

Command History

Release	Modification
11.1(25)IA	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
12.1(5)T	The **availability** and **route-map** metrics were added.

Usage Guidelines

Use host-specific weights when you want to use different metric weights for different virtual host names (for example, www.xyz.com and ftp.xyz.com).

The new availability metric allows the DistributedDirector to attempt to create a TCP connection to each distributed server on a configured port over a configurable time interval.

If desired, host-specific weights can instead be configured on the DistributedDirector default DNS server.

For example, you could configure host-specific weights with the following DNS TXT record:

```
hostname in txt "ciscoDD: weights {[drp-int number] [drp-ext number] [drp-ser number]
[random number] [admin number]}"
```

To use the default weights for all metrics associated with this host name, use the **no ip director host weights** command. To use the default weights for a specific metric or metrics, use the **no ip director host** *host-name* **weights** [**drp-int** *number*] [**drp-ext** *number*] [**drp-ser** *number*] [**drp-rtt** *number*] [**random** *number*] [**admin** *number*] [**portion** *number*] [**availability** *number*] [**route-map** *number*] command.

Examples

The following example sets the DRP internal metric to 4:

```
Router(config)# ip director host www.xyz.com weights drp-int 4
```

Related Commands

Command	Description
ip director default-weights	Configures default weight metrics for the DistributedDirector.
show ip director dfp	Displays information about the current status of the DistributedDirector connections with a particular DFP agent.

ip director server availability

To configure a default availability value for all ports on a server, use the **ip director server availability** command in global configuration mode. To restore the default, use the **no** form of this command.

ip director server *ip-address* **availability** {*availability-value* | **dfp** [*availability-value*]}

no ip director server *ip-address* **availability** {*availability-value* | **dfp** [*availability-value*]}

Syntax Description

ip-address	IP address.
availability-value	Availability value as it would be represented on the DistributedDirector system. The range is 0 to 65,535.
dfp [*availability-value*]	Availability value as it would be represented on the LocalDirector system. The range for value is 0 to 65,535.

Defaults

The availability default value is 65,535.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

There are two methods for specifying a default availability value. These two methods exist because the LocalDirector and the DistributedDirector deal with values in two different ways. All metrics for the DistributedDirector are arranged such that lower is better; however the LocalDirector load information is calculated such that higher is better. Thus, the DistributedDirector translates the metric value upon receipt from the LocalDirector by subtracting the availability from the maximum possible value of 65,535.

Examples

To configure a default availability to be used if there is no other valid availability information, the following configuration would suffice. The following example shows how to specify the LocalDirector load and DistributedDirector availability, respectively:

```
ip director server 10.0.0.1 availability dfp 1
ip director server 10.0.0.1 availability 65534
```

To make the availability clear and to allow for specifying numbers in both schemes easily, there are two methods of specifying availability information. If the servers are running multiple serves, it may be necessary to configure the default availability value on a per-port basis by using the **ip director server port availability** command.

```
ip director server 10.0.0.1 port availability dfp 65535
ip director server 10.0.0.20 port availability dfp 65535
```

Related Commands

Command	Description
ip director server port availability	Configures a default availability value for a specific port on a server.

ip director server port availability

To configure a default availability value for a specific port on a server, use the **ip director server port availability** command in global configuration mode. To restore the default, use the **no** form of this command.

ip director server *ip-address* **port availability** {*availability-value* | **dfp** [*availability-value*]}

no ip director server *ip-address* **port availability** {*availability-value* | **dfp** [*availability-value*]}

Syntax Description

ip-address	IP address.
availability-value	Availability value as it would be represented on the DistributedDirector system. The range is 0 to 65,535.
dfp [*availability-value*]	Availability value as it would be represented on the LocalDirector system. The range for value is 0 to 65,535.

Defaults

The availability default value is 65,535.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

There are two methods for specifying a default availability value. These two methods exist because the LocalDirector and the DistributedDirector deal with values in two different ways. All metrics for the DistributedDirector are arranged such that lower is better; however the LocalDirector load information is calculated such that higher is better. Thus, the DistributedDirector translates the metric value upon receipt from the LocalDirector by subtracting the availability from the maximum possible value of 65,535.

Examples

To make the availability clear and to allow for specifying numbers in both schemes easily, there are two methods of specifying availability information. If the servers are running multiple serves, it may be necessary to configure the default availability value on a per-port basis by using the **ip director server port availability** command.

```
ip director server 10.0.0.1 port availability dfp 65535
ip director server 10.0.0.20 port availability dfp 65535
```

To configure a default availability to be used if there is no other valid availability information, the following configuration would suffice. The following example shows how to specify the LocalDirector load and DistributedDirector availability, respectively:

```
ip director server 10.0.0.1 availability dfp 1
ip director server 10.0.0.1 availability 65534
```

Related Commands

Command	Description
ip director server availability	Configures a default availability value for all ports on a server.

ip dns server

To enable the Domain Name System (DNS) server on a router, use the **ip dns server** command in global configuration mode. To disable the DNS server, use the **no** form of the command.

ip dns server

no ip dns server

Syntax Description

This command has no arguments or keywords.

Defaults

The DNS server is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

Use the command to enable the DNS server as needed.

Examples

In the following example, the DNS server is enabled:

```
Router(config)# ip dns server
```

ip drp domain

To add a new domain to the DistributedDirector client or to configure an existing domain, use the **ip drp domain** command in global configuration mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

ip drp domain *domain-name*

no ip drp domain *domain-name*

Syntax Description

domain-name	Specified domain name.

Defaults

No default domain is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

The **ip drp domain** command can be used only on a Director Response Protocol (DRP) agent. The boomerang client is the DRP agent.

Enabling this command puts the client in boomerang configuration mode.

Use the **ip drp domain** command to enter a new or existing domain name. Entering a new domain name creates a new domain, and entering an existing domain name allows the user to configure the specified domain. When a domain name is configured on the boomerang client, the user can configure specific parameters, such as server address, aliases, and time to live (TTL) values, for that domain.

When a Director Response Protocol (DRP) agent receives a Domain Name System (DNS) racing message from boomerang servers such as DistributedDirector, the DRP agent extracts the specified domain name (for example, www.cisco.com) in the DNS message.

Examples

In the following example, a domain named “www.boom1.com” is added on the boomerang client:

```
Router(config)# ip drp domain www.boom1.com

Router# show running-config
.
.
.
ip drp domain www.boom1.com
```

Related Commands

Command	Description
alias (boomerang)	Configures an alias name for a specified domain.
server (boomerang)	Configures the server address for a specified boomerang domain.
show ip drp	Displays DRP statistics on DistributedDirector or a DRP server agent.
show ip drp boomerang	Displays boomerang information on the DRP agent.
ttl dns	Configures the number of seconds for which an answer received from the boomerang client will be cached by the DNS client.
ttl ip	Configures the IP TTL value for the boomerang response packets sent from the boomerang client to the DNS client in number of hops.

ip finger

To configure a system to accept Finger protocol requests (defined in RFC 742), use the **ip finger** command in global configuration mode. To disable this service, use the **no** form of this command.

ip finger [**rfc-compliant**]

no ip finger

Syntax Description

rfc-compliant	(Optional) Configures the system to wait for "Return" or "/W" input when processing Finger requests. This keyword should not be used for those systems.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.1(5), 12.1(5)T	This command was changed from being enabled by default to being disabled by default.

Usage Guidelines

The Finger service allows remote users to view the output equivalent to the **show users** [**wide**] command.

When **ip finger** is configured, the router will respond to a **telnet** *a.b.c.d* **finger** command from a remote host by immediately displaying the output of the **show users** command and then closing the connection.

When the **ip finger rfc-compliant** command is configured, the router will wait for input before displaying anything (as required by RFC 1288). The remote user can then enter the Return key to display the output of the **show users** EXEC command, or enter **/W** to display the output of the **show users wide** EXEC command. After this information is displayed, the connection is closed.

Note As with all minor services, the Finger service should be disabled on your system if you do not have a need for it in your network.

Any network device that has UDP, TCP, BOOTP, or Finger services should be protected by a firewall or have the services disabled to protect against Denial of Service attacks.

Because of the potential for hung lines, the **rfc-compliant** form of this command should not be configured for devices with more than 20 simultaneous users.

Examples

The following example disables the Finger protocol:

```
Router(config)# no ip finger
```

ip ftp passive

To configure the router to use only passive FTP connections, use the **ip ftp passive** command in global configuration mode. To allow all types of FTP connections, use the **no** form of this command.

ip ftp passive

no ip ftp passive

Syntax Description

This command has no arguments or keywords.

Defaults

All types of FTP connections are allowed.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Examples

In the following example, the router is configured to use only passive FTP connections:

```
Router(config)# ip ftp passive
```

Related Commands

Command	Description
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp source-interface	Specifies the source IP address for FTP connections.
ip ftp username	Configures the username for FTP connections.

ip ftp password

To specify the password to be used for File Transfer Protocol (FTP) connections, use the **ip ftp password** command in global configuration mode. To return the password to its default, use the **no** form of this command.

ip ftp password [*type*] *password*

no ip ftp password

Syntax Description

type	(Optional) Type of encryption to use on the password. A value of 0 disables encryption. A value of 7 indicates proprietary encryption.
password	Password to use for FTP connections.

Defaults

The router forms a password *username@routername.domain*. The variable *username* is the username associated with the current session, *routername* is the configured host name, and *domain* is the domain of the router.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Examples

The following example configures the router to use the username “red” and the password “blue” for FTP connections:

```
Router(config)# ip ftp username red
Router(config)# ip ftp password blue
```

Related Commands

Command	Description
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp source-interface	Specifies the source IP address for FTP connections.
ip ftp username	Configures the username for FTP connections.

ip ftp source-interface

To specify the source IP address for File Transfer Protocol (FTP) connections, use the **ip ftp source-interface** command in global configuration mode. To use the address of the interface where the connection is made, use the **no** form of this command.

ip ftp source-interface *interface*

no ip ftp source-interface

Syntax Description

interface	The interface type and number to use to obtain the source address for FTP connections.

Defaults

The FTP source address is the IP address of the interface the FTP packets use to leave the router.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Use this command to set the same source address for all FTP connections.

Examples

The following example configures the router to use the IP address associated with Ethernet interface 0 as the source address on all FTP packets, regardless of which interface is actually used to send the packet:

```
ip ftp source-interface ethernet 0
```

Related Commands

Command	Description
ip ftp passive	Configures the router to use only passive FTP connections
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp username	Configures the username for FTP connections.

ip ftp username

To configure the username for File Transfer Protocol (FTP) connections, use the **ip ftp username** command in global configuration mode. To configure the router to attempt anonymous FTP, use the **no** form of this command.

ip ftp username *username*

no ip ftp username

Syntax Description

username	Username for FTP connections.

Defaults

The Cisco IOS software attempts an anonymous FTP.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The remote username must be associated with an account on the destination server.

Examples

In the following example, the router is configured to use the username "red" and the password "blue" for FTP connections:

```
Router(config)# ip ftp username red
Router(config)# ip ftp password blue
```

Related Commands

Command	Description
ip ftp passive	Configures the router to use only passive FTP connections.
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp source-interface	Specifies the source IP address for FTP connections.

ip http access-class

To specify the access list that should be used to restrict access to the HTTP server, use the **ip http access-class** command in global configuration mode. To remove a previously configured access list association, use the **no** form of this command.

ip http access-class *access-list-number*

no ip http access-class *access-list-number*

Syntax Description

access-list-number	Standard IP access list number in the range 0 to 99, as configured by the **access-list** global configuration command.

Defaults

No access list is applied to the HTTP server.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

If this command is configured, the specified access list is assigned to the HTTP server. Before the HTTP server accepts a connection, it checks the access list. If the check fails, the HTTP server does not accept the request for a connection.

Examples

In the following example the access list identified as "20" is defined and assigned to the HTTP server:

```
Router(config)# ip access-list standard 20
Router(config-std-nacl)# permit 209.165.202.0 0.0.0.255
Router(config-std-nacl)# permit 209.165.0.0 0.0.255.255
Router(config-std-nacl)# permit 209.0.0.0 0.255.255.255
! (Note: all other access implicitly denied)
Router(config-std-nacl)# exit
Router(config)# ip http access-class 20
```

Related Commands

Command	Description
ip access-list	Assigns an ID to an access list and enters access list configuration mode.
ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface.

ip http authentication

To specify a particular authentication method for HTTP server users, use the **ip http authentication** command in global configuration mode. To disable a configured authentication method, use the **no** form of this command.

ip http authentication {**aaa** | **enable** | **local** | **tacacs**}

no ip http authentication {**aaa** | **enable** | **local** | **tacacs**}

Syntax Description

aaa	Indicates that the authentication method used for the AAA login service should be used for authentication. The AAA login service method is specified by the **aaa authentication login default** command.
enable	Indicates that the "enable" password should be used for authentication. (This is the default method.)
local	Indicates that the login user name, password and privilege level access combination specified in the local system configuration (by the **username** global configuration command) should be used for authentication and authorization.
tacacs	Indicates that the TACACS (or XTACACS) server should be used for authentication.

Defaults

The "enable" password is required when users (clients) connect to the HTTP server.

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.3(8)	The **tacacs** keyword was removed.

Usage Guidelines

The **ip http authentication** command specifies the authentication method to be used for login when a client connects to the HTTP server. Use of the **ip http authentication aaa** command option is recommended. The **enable**, **local**, and **tacacs** methods should be specified using the **aaa authentication login** command.

The "enable" password method is the default HTTP server authentication method. If the enable password is used as the HTTP server login authentication method, the client connects to the HTTP server with a default privilege level of 15.

Note When the "enable" password is used as the HTTP server login authentication method, any username entered will be ignored; the server will only verify the "enable" password. This may make it easier for an attacker to access the router. Because a username and password pair is more secure than using only a password for authentication, using only "enable" password for authentication is strongly discouraged.

Instead, use of the **local** or **tacacs** authentication options, configured as part of a global Authentication, Authorization, and Accounting (AAA) framework, is recommended.
To configure HTTP access as part of a AAA policy, use the **ip http authentication aaa** command option. The “local”, “tacacs”, or “enable” authentication methods should then be configured using the **aaa authentication login** command.

For information about adding users into the local username database, refer to the *Cisco IOS Security Configuration Guide*.

Examples

The following example specifies that the method configured for AAA should be used for authentication for HTTP server users. The AAA login method is configured as the “local” username/password authentication method.

```
Router(config)# ip http authentication aaa
Router(config)# aaa authentication login default local
```

Related Commands

Command	Description
ip http server	Enables the HTTP server.
aaa authentication login	Specifies the login authentication method to be used by the authentication, authorization, and accounting (AAA) service.

ip http client secure-ciphersuite

To specify the CipherSuite that should be used for encryption over the secure HTTP connection from the client to a remote server, use the **ip http client secure-ciphersuite** command in global configuration mode. To remove a previously configured CipherSuite specification for the client, use the **no** form of this command.

ip http client secure-ciphersuite {[**3des-ede-cbc-sha**] [**rc4-128-sha**] [**rc4-128-md5**] [**des-cbc-sha**]}

no ip http client secure-ciphersuite

Syntax Description

3des-ede-cbc-sha	SSL_RSA_WITH_3DES_EDE_CBC_SHA—RSA key exchange with 3DES and DES-EDE3-CBC for message encryption and SHA for message digest.
rc4-128-sha	SSL_RSA_WITH_RC4_128_SHA—RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and SHA for message digest.
rc4-128-md5	SSL_RSA_WITH_RC4_128_MD5—RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and MD5 for message digest.
des-cbc-sha	SSL_RSA_WITH_DES_CBC_SHA—RSA key exchange with DES-CBC for message encryption and SHA for message digest.

Defaults

The client and server negotiate the best CipherSuite that they both support from the list of available CipherSuites.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

This command allows you to restrict the list of CipherSuites (encryption algorithms) that the client offers when connecting to a secure HTTP server. For example, you may want to allow only the most secure CipherSuite(s) to be used.

Unless you have a reason to specify the CipherSuites that should be used, or you are unfamiliar with the details of these CipherSuites, you should leave this command unconfigured and let the server and client negotiate the CipherSuite that they both support (this is the default). The **no** form of this command returns the list of available CipherSuites to the default (that is, all CipherSuites supported on your device are available for negotiation).

Examples

In the following example the HTTPS client is configured to use only the SSL_RSA_WITH_3DES_EDE_CBC_SHA CipherSuite:

```
Router(config)# ip http client secure-ciphersuite 3des-ede-cbc-sha
```

Related Commands

Command	Description
show ip http client secure status	Displays the configuration status of the secure HTTP client.

ip http client secure-trustpoint

To specify the remote Certificate of Authority (CA) trustpoint that should be used if certification is needed for the secure HTTP client, use the **ip http client secure-trustpoint** command in global configuration mode. To remove a client trustpoint from the configuration, use the **no** form of this command.

ip http client secure-trustpoint *trustpoint-name*

no ip http client secure-trustpoint *trustpoint-name*

Syntax Description

trustpoint-name	Name of a configured trustpoint. Use the same trustpoint name that was used in the associated **crypto ca trustpoint** command.

Defaults

If the remote HTTPS server requests client certification, the secure HTTP client will use the trustpoint configured as **primary** in the CA trustpoint configuration.

If a trustpoint is not configured, client certification will fail.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

This command specifies that the secure HTTP client should use the certificate associated with the trustpoint indicated by the *trustpoint-name* argument. Use the same trustpoint name that you used in the associated **crypto ca trustpoint** command.

The specified X.509v3 security certificate will be used by the secure HTTP (HTTPS) client for cases when the remote HTTPS server requires client authorization.

Use of this command assumes you have already declared a CA trustpoint using the **crypto ca trustpoint** command and associated sub-mode commands. If the remote HTTPS server requires client authorization and a trustpoint is not configured for the client, the remote HTTPS server will reject the connection.

If this command is not used, the client will attempt to use the certificate associated with the primary trustpoint. The primary trustpoint is configured using the **primary** CA TrustPoint configuration mode command.

Examples

In the following example the CA trustpoint is configured then referenced in the secure HTTP server configuration:

```
!The following commands specifies a CA trustpoint that can be used
!to obtain a X.509v3 security certificate.
Router(config)# crypto ca trustpoint tp1
Router(config-ca)# enrollment url http://host1:80
Router(config-ca)# exit
```

```
!The following command is used to actually obtain the security certificate.
!A trustpoint NAME is used because there could be multiple trust points
!configured for the router.
Router(config)# crypto ca enrollment TP1
!The following command specifies that the secure HTTP client
!should use the certificate associated with the TP1 trustpoint for HTTPS connections.
Router(config)# ip http client secure-trustpoint tp1
```

Related Commands

Command	Description
crypto ca trustpoint	Specifies a name for a certificate authority trustpoint and enters CA TrustPoint configuration mode.
primary	Indicates that the CA trustpoint being configured should be used as the primary (default) trustpoint.

ip http max-connections

To configure the maximum number of concurrent connections allowed for the HTTP server, use the **ip http max-connections** command in global configuration mode. To return the maximum connection value to the default, use the **no** form of this command.

ip http max-connections *value*

no ip http max-connections *value*

Syntax Description

value	The maximum number of concurrent HTTP connections. The range is 1 to 16. The default is 5.

Defaults

5 concurrent HTTP connections.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Platform-specific implementations can supersede the upper range limit of 16.

If a new value is configured that is less than the previously configured value while the current number of connections exceeds the new maximum value, the HTTP server will not abort any of the current connections. However, the server will not accept any new connections until the current number of connections falls below the new configured value.

Examples

In the following example the HTTP server is configured to allow up to 10 simultaneous connections:

```
Router(config)# ip http server
Router(config)# ip http max-connections 10
```

Related Commands

Command	Description
ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface.

ip http path

To specify the base path used to locate files for use by the HTTP server, use the **ip http path** command in global configuration mode. To disable the HTTP server, use the **no** form of this command.

ip http path *url*

no ip http path *url*

Syntax Description

url	Cisco IOS File System (IFS) Uniform Resource Locator (URL) specifying the location of the HTML files used by the HTTP server.

Defaults

The HTTP server is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

After enabling the HTTP server, you should set the base path by specifying the location of the HTML files to be served. HTML files used by the HTTP web server typically reside in system Flash memory.

Remote URLs can be specified using this command, but use of remote path names (for example, where HTML files are located on a remote TFTP server) is not recommended.

Examples

In the following example, the HTML files are located in the default Flash location on the system:

```
Router(config)# ip http path flash:
```

In the following example, the HTML files are located in the directory named web on the Flash memory card inserted in slot 0:

```
Router(config)# ip http path slot0:web
```

Related Commands

Command	Description
ip http server	Enables the HTTP server, including the Cisco web browser user interface.

ip http port

To specify the port number to be used by the HTTP server, use the **ip http port** command in global configuration mode. To return the port number to the default, use the **no** form of this command.

ip http port *port-number*

no ip http port *port-number*

Syntax Description

port-number	The port number to be used for the HTTP server. Valid values are 80 or any value from 1024 to 65535. The default is 80.

Defaults

The HTTP server uses port 80.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(15)T	This command was modified to restrict port numbers. The port number 443 is now reserved for HTTPS (HTTP over SSL) connections.

Usage Guidelines

HTTP port 80 is the standard port used by web servers.

Examples

In the following example the HTTP server port is changed to port 8080.

```
Router(config)# ip http server
Router(config)# ip http port 8080
```

Related Commands

Command	Description
ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface.

ip http secure-ciphersuite

To specify the CipherSuites that should be used by the secure HTTP server when negotiating a connection with a remote client, use the **ip http secure-ciphersuite** command in global configuration mode. To return the configuration to the default set of CipherSuites, use the **no** form of this command.

ip http secure-ciphersuite {[**3des-ede-cbc-sha**] [**rc4-128-sha**] [**rc4-128-md5**] [**des-cbc-sha**]}

no ip http secure-ciphersuite

Syntax Description

3des-ede-cbc-sha	SSL_RSA_WITH_3DES_EDE_CBC_SHA—RSA key exchange with 3DES and DES-EDE3-CBC for message encryption and SHA for message digest.
rc4-128-sha	SSL_RSA_WITH_RC4_128_SHA —RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and SHA for message digest.
rc4-128-md5	SSL_RSA_WITH_RC4_128_MD5 —RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and MD5 for message digest.
des-cbc-sha	SSL_RSA_WITH_DES_CBC_SHA—RSA key exchange with DES-CBC for message encryption and SHA for message digest.

Defaults

The HTTPS server negotiates the best CipherSuite using the list received from connecting client.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

This command is used to restrict the list of CipherSuites (encryption algorithms) that should be used for encryption over the HTTPS connection. For example, you may want to allow only the most secure CipherSuite(s) to be used.

Unless you have a reason to specify the CipherSuites that should be used, or you are unfamiliar with the details of these CipherSuites, you should leave this command unconfigured and let the server and client negotiate the CipherSuite that they both support (this is the default).

The supported CipherSuites vary by Cisco IOS software image. For example, “IP Sec56” (“k8”) images support only the SSL_RSA_WITH_DES_CBC_SHA CipherSuite in Cisco IOS Release 12.2T.

In terms of router processing load (speed), the following list ranks the CipherSuites from fastest to slowest (slightly more processing time is required for the more secure and more complex CipherSuites) :

1. SSL_RSA_WITH_DES_CBC_SHA
2. SSL_RSA_WITH_RC4_128_MD5

3. SSL_RSA_WITH_RC4_128_SHA
4. SSL_RSA_WITH_3DES_EDE_CBC_SHA

Additional information about these CipherSuites can be found online from sources that document the Secure Socket Layer (SSL) 3.0 protocol.

Examples

The following example restricts the CipherSuites offered to a connecting secure web client:

```
Router(config)# ip http secure-ciphersuite rc4-128-sha rc4-128-md5
```

Related Commands

Command	Description
ip http secure-server	Enables the secure HTTP (HTTPS) server.
show ip http server secure status	Displays the configuration status of the secure HTTP server.

ip http secure-client-auth

To configure the secure HTTP server to authenticate connecting clients, use the **ip http secure-client-auth** command in global configuration mode. To remove the requirement for client authorization, use the **no** form of this command.

ip http secure-client-auth

no ip http secure-client-auth

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled (that is, client authentication is not required for connections to the secure HTTP server).

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

This command configures the HTTP server to request an X.509v3 certificate from the client in order to authenticate the client during the connection process.

In the default connection and authentication process, the client requests a certificate from the HTTP server, but the server does not attempt to authenticate the client. Authenticating the client provides more security than server authentication by itself, but not all web clients may be configured for certificate authority (CA) authentication.

Examples

In the following example the secure web server is enabled and the server is configured to accept connections only from clients with a signed security certificate:

```
Router(config)# no ip http server
Router(config)# ip http secure-server
Router(config)# ip http secure-client-auth
```

Related Commands

Command	Description
ip http secure-server	Enables the secure HTTP (HTTPS) server.
show ip http server secure status	Displays the configuration status of the secure HTTP server.

ip http secure-port

To specify the port (socket) to be used for connections to the secure HTTP (HTTPS) server, use the **ip http secure-port** command in global configuration mode. To return the secure HTTP server port number to the default, use the **no** form of this command.

ip http secure-port *port-number*

no ip http secure-port

Syntax Description

port-number	Port number that should be used for the secure HTTP server. The default port number is 443. Valid options are 443 or any number in the range 1025 to 65535.

Defaults

Port 443

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Examples

The following example changes the port for HTTPS server connections from 443 to 1025:

```
Router(config)# ip http secure-port 1025
```

Related Commands

Command	Description
ip http secure-server	Enables the secure HTTP (HTTPS) server.

ip http secure-server

To enable the secure HTTP web server, use the **ip http secure-server** command in global configuration mode. To disable the secure HTTP server, use the **no** form of this command.

ip http secure-server

no ip http secure-server

Syntax Description

This command has no arguments or keywords.

Defaults

The secure HTTP server is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

The secure HTTP server (also called the HTTPS server) uses the Secure Socket Layer (SSL) version 3.0 protocol.

Note When enabling the secure HTTP server you should always disable the standard HTTP server to prevent insecure connections to the same services. Disable the standard HTTP server using the **no ip http server** command in global configuration mode (this is a precautionary step; typically, the HTTP server is disabled by default).

If a certificate authority is to be used for certification, you should declare the CA trustpoint on the routing device before enabling the secure HTTP server.

Examples

In the following example the secure HTTP server is enabled, and the (previously configured) CA trustpoint `CA_trust_local` is specified:

```
Router# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip http secure-server
Router(config)# ip http secure-trustpoint CA_trust_local
Router(config)# end
Router# show ip http server secure status
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-12a
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint: CA_trust_local
```

Related Commands

Command	Description
ip http secure-trustpoint	Specifies the CA trustpoint that should be used for obtaining signed certificates for the secure HTTP server.
show ip http server secure status	Displays the configuration status of the secure HTTP server.

ip http secure-trustpoint

To specify the certificate authority (CA) trustpoint that should be used for obtaining signed certificates for the secure HTTP server, use the **ip http secure-trustpoint** command in global configuration mode. To remove a previously specified CA trustpoint, use the **no** form of this command.

ip http secure-trustpoint *trustpoint-name*

no ip http secure-trustpoint *trustpoint-name*

Syntax Description

trustpoint-name	Name of a configured trustpoint. Use the same trustpoint name that was used in the associated **crypto ca trustpoint** command.

Defaults

The secure HTTP server will use the trustpoint configured as **primary** in the CA trustpoint configuration.

If a trustpoint is not configured, the secure HTTP server will use a self-signed certificate.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

This command specifies that the secure HTTP server should use the X.509v3 certificate associated with the trustpoint indicated by the *trustpoint-name* argument. Use the same trustpoint name that you used in the associated **crypto ca trustpoint** command.

The specified X.509v3 security certificate will be used to authenticate the server to connecting clients, and, if remote client authentication is enabled, to authenticate the connecting clients.

Use of this command assumes you have already declared a CA trustpoint using the **crypto ca trustpoint** command and associated sub-mode commands. If a trustpoint is not configured, the secure HTTP server will use a self-signed certificate.

If this command is not used, the server will attempt to use the certificate associated with the primary trustpoint. The primary trustpoint is configured using the **primary** CA TrustPoint configuration mode command.

Examples

In the following example the CA trustpoint is configured, a certificate is obtained, then the certificate is referenced in the secure HTTP server configuration:

```
!The following commands specifies a CA trustpoint that can be used
!to obtain a X.509v3 security certificate.
!A trustpoint NAME is used because there could be multiple trustpoints
!configured for the router.
Router(config)# crypto ca trustpoint tp1
Router(config-ca)# enrollment url http://host1:80
```

```
Router(config-ca)# exit
Router(config)# crypto ca authenticate tp1
!The following command is used to actually obtain the security certificate.
Router(config)# crypto ca enrollment tp1
Router(config)# ip http secure-server
!The following command specifies that the secure HTTP server
!should use a certificate associated with the TP1 trustpoint for HTTPS connections.
Router(config)# ip http secure-trustpoint tp1
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the certificate authority (CA) that your routing device should use.
ip http secure-server	Enables the secure HTTP (HTTPS) server.
show ip http server secure status	Displays the configuration status of the secure HTTP server.

ip http server

To enable the HTTP server on your system, including the Cisco web browser user interface, use the **ip http server** command in global configuration mode. To disable the HTTP server, use the **no** form of this command.

ip http server

no ip http server

Syntax Description

This command has no arguments or keywords.

Defaults

The HTTP server is disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(15)T	The HTTP 1.0 implementation was replaced by the HTTP 1.1 implementation. The secure HTTP server feature was added.

Usage Guidelines

The HTTP server uses the standard port 80 by default.

Caution The standard HTTP server and the secure HTTP server can run at the same time on your system. If you enable the secure HTTP server using the **ip http secure-server** command, you should disable the standard HTTP server using the **no ip http server** command to ensure that secure data cannot be accessed through the standard HTTP connection.

Examples

In the following example the HTTP server is enabled:

```
Router(config)# ip http server
Router(config)# ip http path flash:
```

Related Commands

Command	Description
ip http path	Specifies the base path used to locate files for use by the HTTP server.
ip http secure-server	Enables the secure HTTP server.

ip http timeout-policy

To configure the parameters for closing connections to the local HTTP server, use the **ip http timeout-policy** command in global configuration mode. To return the parameters to their defaults, use the **no** form of this command.

ip http timeout-policy idle *seconds* **life** *seconds* **requests** *value*

no ip http timeout-policy

Syntax Description

idle *seconds*	The maximum number of seconds the connection will be kept open if no data is received or response data cannot be sent out on the connection. The valid range is from 1 to 600 seconds (10 minutes). The default value is 180 seconds (3 minutes).
life *seconds*	The maximum number of seconds the connection will be kept open, from the time the connection is established. The valid range is from 1 to 86400 seconds (24 hours). The default value is 180 seconds (3 minutes).
requests *value*	The maximum limit on the number of requests processed on a persistent connection before it is closed. The valid range is from 1 to 86400. The default value is 1.

Defaults

HTTP server connection idle time: 180 seconds (3 minutes)

HTTP server connection life time: 180 seconds (3 minutes)

HTTP server connection maximum requests: 1

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

This command sets the characteristics that determine how long a connection to the HTTP server should remain open.

This command may not take effect immediately on any HTTP connections that are open at the time you use this command. In other words, new values for idle time, life time, and maximum requests will apply only to connections made to the HTTP server after this command is issued.

A connection may be closed sooner than the configured **idle** time if the server is too busy or the limit on the **life** time or the number of **requests** is reached.

A connection may be closed sooner than the configured **life** time if the server is too busy or the limit on the **idle** time or the number of **requests** is reached. Also, since the server will not close a connection while actively processing a request, the connection may remain open longer than the specified **life** time if processing is occurring when the life maximum is reached. In this case, the connection will be closed when processing finishes.

A connection may be closed before the maximum number of requests are processed if the server is too busy or the limit on the **idle** time or **life** time is reached.

The **ip http timeout-policy** command allows you to specify a general access policy to the HTTP server by adjusting the connection timeout values. For example, if you want to maximize throughput for HTTP connections, you should configure a policy that minimizes connection overhead. You can do this by specifying large values for the **life** and **request** options so that each connection stays open longer and more requests are processed for each connection.

Another example would be to configure a policy that minimizes the response time for new connections. You can do this by specifying small values for the **life** and **request** options so that the connections are quickly released to serve new clients.

A throughput policy would be better for HTTP sessions with dedicated management applications, as it would allow the application to send more requests before the connection is closed, while a response time policy would be better for interactive HTTP sessions, as it would allow more people to connect to the server at the same time without having to wait for connections to become available.

In general, you should configure these options as appropriate for your environment. The value for the **idle** option should be balanced so that it is large enough not to cause an unwanted request or response timeout on the connection, but small enough that it does not hold a connection open longer than necessary.

Examples

In the following example, a Throughput timeout policy is applied. This configuration would allow each connection to be idle a maximum of 30 seconds (approximately). Each connection will remain open (be "alive") until either the HTTP server has been busy processing requests for approximately 2 minutes (120 seconds) or until approximately 100 requests have been processed.

```
Router(config)# ip http timeout-policy idle 30 life 120 requests 100
```

In the following example, a Response Time timeout policy is applied. This configuration would allow each connection to be idle a maximum of 30 seconds (approximately). Each connection will be closed as soon as the first request has been processed.

```
Router(config)# ip http timeout-policy idle 30 life 30 requests 1
```

Related Commands

Command	Description
ip http server	Enables the HTTP server, including the Cisco web browser user interface.

ip rarp-server

To enable the router to act as a Reverse Address Resolution Protocol (RARP) server, use the **ip rarp-server** command in interface configuration mode. To restore the interface to the default of no RARP server support, use the **no** form of this command.

ip rarp-server *ip-address*

no ip rarp-server *ip-address*

Syntax Description

ip-address	IP address that is to be provided in the source protocol address field of the RARP response packet. Normally, this is set to whatever address you configure as the primary address for the interface.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This feature makes diskless booting of clients possible between network subnets where the client and server are on separate subnets.

RARP server support is configurable on a per-interface basis, so that the router does not interfere with RARP traffic on subnets that need no RARP assistance.

The Cisco IOS software answers incoming RARP requests only if both of the following two conditions are met:

- The **ip rarp-server** command has been configured for the interface on which the request was received.
- A static entry is found in the IP ARP table that maps the MAC address contained in the RARP request to an IP address.

Use the **show ip arp** EXEC command to display the contents of the IP ARP cache.

Sun Microsystems, Inc. makes use of RARP and UDP-based network services to facilitate network-based booting of SunOS on it's workstations. By bridging RARP packets and using both the **ip helper-address** interface configuration command and the **ip forward-protocol** global configuration command, the Cisco IOS software should be able to perform the necessary packet switching to enable booting of Sun workstations across subnets. Unfortunately, some Sun workstations assume that the sender of the RARP response, in this case the router, is the host that the client can contact to TFTP load the bootstrap image. This causes the workstations to fail to boot.

By using the **ip rarp-server** command, the Cisco IOS software can be configured to answer these RARP requests, and the client machine should be able to reach its server by having its TFTP requests forwarded through the router that acts as the RARP server.

In the case of RARP responses to Sun workstations attempting to diskless boot, the IP address specified in the **ip rarp-server** interface configuration command should be the IP address of the TFTP server. In addition to configuring RARP service, the Cisco IOS software must be configured to forward UDP-based Sun portmapper requests to completely support diskless booting of Sun workstations. This can be accomplished using configuration commands of the following form:

```
ip forward-protocol udp 111
interface interface name
ip helper-address target-address
```

RFC 903 documents the RARP.

Examples

The following partial example configures a router to act as a RARP server. The router is configured to use the primary address of the specified interface in its RARP responses.

```
arp 172.30.2.5 0800.2002.ff5b arpa
interface ethernet 0
ip address 172.30.3.100 255.255.255.0
ip rarp-server 172.30.3.100
```

In the following example, a router is configured to act as a RARP server, with TFTP and portmapper requests forwarded to the Sun server:

```
! Allow the router to forward broadcast portmapper requests
ip forward-protocol udp 111
! Provide the router with the IP address of the diskless sun
arp 172.30.2.5 0800.2002.ff5b arpa
interface ethernet 0
! Configure the router to act as a RARP server, using the Sun Server's IP
! address in the RARP response packet.
ip rarp-server 172.30.3.100
! Portmapper broadcasts from this interface are sent to the Sun Server.
ip helper-address 172.30.3.100
```

Related Commands

Command	Description
ip forward-protocol	Speeds up flooding of UDP datagrams using the spanning-tree algorithm.
ip helper-address	Forwards UDP broadcasts, including BOOTP, received on an interface.

ip rcmd domain-lookup

To reenable the basic Domain Name Service (DNS) security check for rcp and rsh, use the **ip rcmd domain-lookup** command in global configuration mode. To disable the basic DNS security check for remote copy protocol (rcp) and remote shell protoco (rsh), use the **no** form of this command.

ip rcmd domain-lookup

no ip rcmd domain-lookup

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The abbreviation RCMD (remote command) is used to indicate both rsh and rcp.

DNS lookup for RCMD is enabled by default (provided general DNS services are enabled on the system using the **ip domain-lookup** command).

The **no ip rcmd domain-lookup** command is used to disable the DNS lookup for RCMD. The **ip rcmd domain-lookup** command is used to reenable the DNS lookup for RCMD.

DNS lookup for RCMD is performed as a basic security check. This check is performed using a host authentication process. When enabled, the system records the address of the requesting client. That address is mapped to a host name using DNS. Then a DNS request is made for the IP address for that host name. The IP address received is then checked against the original requesting address. If the address does not match with any of the addresses received from DNS, the RCMD request will not be serviced.

This reverse lookup is intended to help protect against spoofing. However, please note that the process only confirms that the IP address is a valid “routable” address; it is still possible for a hacker to spoof the valid IP address of a known host.

The DNS lookup is done after the TCP handshake but before the router (which is acting as a rsh/rcp server) sends any data to the remote client.

The **no ip rcmd domain-lookup** will turn off DNS lookups for rsh and rcp only. The **no ip domain-lookup** command takes precedence over the **ip rcmd domain-lookup** command. This means that if the **no ip domain-lookup** command is in the current configuration, DNS will be bypassed for rcp and rsh even if the **ip rcmd domain-lookup** command is enabled.

Examples

In the following example, the DNS security check is disabled for RCMD (rsh/rcp):

```
Router(config)# no ip rcmd domain-lookup
```

Related Commands

Command	Description
ip domain-lookup	Enables the IP DNS-based host name-to-address translation.

ip rcmd rcp-enable

To configure the Cisco IOS software to allow remote users to copy files to and from the router using remote copy protocol (rcp), use the **ip rcmd rcp-enable** command in global configuration mode. To disable rcp on the device, use the **no** form of this command.

ip rcmd rcp-enable

no ip rcmd rcp-enable

Syntax Description

This command has no arguments or keywords.

Defaults

To ensure security, the router is not enabled for rcp by default.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

To allow a remote user to execute rcp commands on the router, you must also create an entry for the remote user in the local authentication database using the **ip rcmd remote-host** command.

The **no ip rcmd rcp-enable** command does not prohibit a local user from using rcp to copy system images and configuration files to and from the router.

To protect against unauthorized users copying the system image or configuration files, the router is not enabled for rcp by default.

Examples

In the following example, the rcp service is enabled on the system, the IP address assigned to the Loopback0 interface is used as the source address for outbound rcp and rsh packets, and access is granted to the user “netadmin3”on the remote host 172.16.101.101:

```
Router(config)# ip rcmd rcp-enable
Router(config)# ip rcmd source-interface Loopback0
Router(config)# ip rcmd remote-host router1 172.16.101.101 netadmin3
```

Related Commands

Command	Description
ip rcmd remote-host	Creates an entry for the remote user in a local authentication database so that remote users can execute commands on the router using rsh or rcp.

ip rcmd remote-host

To create an entry for the remote user in a local authentication database so that remote users can execute commands on the router using remote shell protocol (rsh) or remote copy protocol (rcp), use the **ip rcmd remote-host** command in global configuration mode. To remove an entry for a remote user from the local authentication database, use the **no** form of this command.

ip rcmd remote-host *local-username* {*ip-address* | *host-name*} *remote-username* [**enable** [*level*]]

no ip rcmd remote-host *local-username* {*ip-address* | *host-name*} *remote-username* [**enable** [*level*]]

Syntax Description

local-username	Name of the user on the local router. You can specify the router name as the username. This name needs to be communicated to the network administrator or to the user on the remote system. To be allowed to remotely execute commands on the router, the remote user must specify this value correctly.
ip-address	IP address of the remote host from which the local router will accept remotely executed commands. Either the IP address or the host name is required.
host-name	Name of the remote host from which the local router will accept remotely executed commands. Either the host name or the IP address is required.
remote-username	Name of the user on the remote host from which the router will accept remotely executed commands.
enable [*level*]	(Optional) Enables the remote user to execute privileged EXEC commands using rsh or to copy files to the router using rcp. The range is from 1 to 15. The default is 15. For information on the enable level, refer to the **privilege level** global configuration command in the *Cisco IOS Security Command Reference*.

Defaults

No entries are in the local authentication database.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

A TCP connection to a router is established using an IP address. Using the host name is valid only when you are initiating an rcp or rsh command from a local router. The host name is converted to an IP address using DNS or host-name aliasing.

To allow a remote user to execute rcp or rsh commands on a local router, you must create an entry for the remote user in the local authentication database. You must also enable the router to act as an rsh or rcp server.

To enable the router to act as an rsh server, issue the **ip rcmd rsh-enable** command. To enable the router to act as an rcp server, issue the **ip rcmd rcp-enable** command.The router cannot act as a server for either of these protocols unless you explicitly enable the capacity.

A local authentication database, which is similar to a UNIX *.rhosts* file, is used to enforce security on the router through access control. Each entry that you configure in the authentication database identifies the local user, the remote host, and the remote user. To permit a remote user of rsh to execute commands in privileged EXEC mode or to permit a remote user of rcp to copy files to the router, specify the **enable** keyword and level. For information on the enable level, refer to the **privilege level** global configuration command in the *Cisco IOS Security Command Reference*.

An entry that you configure in the authentication database differs from an entry in a UNIX *.rhosts* file in the following aspect. Because the *.rhosts* file on a UNIX system resides in the home directory of a local user account, an entry in a UNIX *.rhosts* file need not include the local username; the local username is determined from the user account. To provide equivalent support on a router, specify the local username along with the remote host and remote username in each authentication database entry that you configure.

For a remote user to be able to execute commands on the router in its capacity as a server, the local username, host address or name, and remote username sent with the remote client request must match values configured in an entry in the local authentication file.

A remote client host should be registered with DNS. The Cisco IOS software uses DNS to authenticate the remote host's name and address. Because DNS can return several valid IP addresses for a host name, the Cisco IOS software checks the address of the requesting client against all of the IP addresses for the named host returned by DNS. If the address sent by the requester is considered invalid, that is, it does not match any address listed with DNS for the host name, then the software will reject the remote-command execution request.

Note that if no DNS servers are configured for the router, then that device cannot authenticate the host in this manner. In this case, the Cisco IOS software sends a broadcast request to attempt to gain access to DNS services on another server. If DNS services are not available, you must use the **no ip domain-lookup** command to disable the attempt to gain access to a DNS server by sending a broadcast request.

If DNS services are not available and, therefore, you bypass the DNS security check, the software will accept the request to remotely execute a command only if all three values sent with the request match exactly the values configured for an entry in the local authentication file.

Examples

The following example allows the remote user *named netadmin3* on a remote host with the IP address 172.16.101.101 to execute commands on *router1* using the rsh or rcp protocol. User netadmin3 is allowed to execute commands in privileged EXEC mode.

```
Router(config)# ip rcmd remote-host router1 172.16.101.101 netadmin3 enable
```

Related Commands

Command	Description
ip rcmd rcp-enable	Configures the Cisco IOS software to allow remote users to copy files to and from the router.

Command	Description
ip domain-lookup	Enables the IP DNS-based host name-to-address translation.
ip rcmd rsh-enable	Configures the router to allow remote users to execute commands on it using the rsh protocol.

ip rcmd remote-username

To configure the remote username to be used when requesting a remote copy using remote copy protocol (rcp), use the **ip rcmd remote-username** command in global configuration mode. To remove from the configuration the remote username, use the **no** form of this command.

ip rcmd remote-username *username*

no ip rcmd remote-username *username*

Syntax Description

username	Name of the remote user on the server. This name is used for rcp copy requests. All files and images to be copied are searched for or written relative to the directory of the remote user's account, if the server has a directory structure, for example, as do UNIX systems.

Defaults

If you do not issue this command, the Cisco IOS software sends the remote username associated with the current tty process, if that name is valid, for rcp copy commands. For example, if the user is connected to the router through Telnet and the user was authenticated through the **username** command, then the software sends that username as the remote username.

Note The remote username must be associated with an account on the destination server.

If the username for the current tty process is not valid, the Cisco IOS software sends the host name as the remote username. For rcp boot commands, the Cisco IOS software sends the access server host name by default.

Note For Cisco, tty lines are commonly used for access services. The concept of tty originated with UNIX. For UNIX systems, each physical device is represented in the file system. Terminals are called tty devices (tty stands for teletype, the original UNIX terminal).

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The rcp protocol requires that a client send the remote username on an rcp request to the server. Use this command to specify the remote username to be sent to the server for an rcp copy request. If the server has a directory structure, as do UNIX systems, all files and images to be copied are searched for or written relative to the directory of the remote user's account.

Note Cisco IOS Release 10.3 added the **ip** keyword to **rcmd** commands. If you are upgrading from Release 10.2 to Release 10.3 or a later release, this keyword is automatically added to any **rcmd** commands you have in your Release 10.2 configuration files.

Examples

The following example configures the remote username to netadmin1:

```
Router(config)# ip rcmd remote-username netadmin1
```

Related Commands

Command	Description
boot network rcp	Changes the default name of the network configuration file from which to load configuration commands.
boot system rcp	Specifies the system image that the router loads at startup.
bridge acquire	Forwards any frames for stations that the system has learned about dynamically.
copy	Copies any file from a source to a destination.

ip rcmd rsh-enable

To configure the router to allow remote users to execute commands on it using remote shell protocol (rsh), use the **ip rcmd rsh-enable** command in global configuration mode. To disable a router that is enabled for rsh, use the **no** form of this command.

ip rcmd rsh-enable

no ip rcmd rsh-enable

Syntax Description

This command has no arguments or keywords.

Defaults

To ensure security, the router is not enabled for rsh by default.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

rsh, used as a client process, gives users the ability to remotely get router information (such as status) without the need to connect into the router and then disconnect. This is valuable when looking at many statistics on many different routers.

Use this command to enable the router to receive rsh requests from remote users. In addition to issuing this command, you must create an entry for the remote user in the local authentication database to allow a remote user to execute rsh commands on the router.

The **no ip rcmd rsh-enable** command does not prohibit a local user of the router from executing a command on other routers and UNIX hosts on the network using rsh. The no form of this command only disables remote access to rsh on the router.

Examples

The following example enables a router as an rsh server:

```
Router(config)# ip rcmd rsh-enable
```

Related Commands

Command	Description
ip rcmd remote-host	Creates an entry for the remote user in a local authentication database so that remote users can execute commands on the router using rsh or rcp.

ip rcmd source-interface

To force remote copy protocol (rcp) or remote shell protocol (rsh) to use the IP address of a specified interface for all outgoing rcp/rsh communication packets, use the **ip rcmd source-interface** command in global configuration mode. To disable a previously configured **ip rcmd source-interface** command, use the **no** form of this command.

ip rcmd source-interface *interface-id*

no ip rcmd source-interface *interface-id*

Syntax Description

interface-id	The name and number used to identify the interface. For example, Loopback2.

Defaults

The address of the interface closest to the destination is used as the source interface for rcp/rsh communications.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

If this command is not used, or if the interface specified in this command is not available (not up), the Cisco IOS software uses the address of the interface closest to the destination as the source address.

Use this command to force the system to tag all outgoing rcp/rsh packets with the IP address associated with the specified interface. This address is used as the source address as long as the interface is in the up state.

This command is especially useful in cases where the router has many interfaces, and you want to ensure that all rcp and/or rsh packets from this router have the same source IP address. A consistent address is preferred so that the other end of the connection (the rcp/rsh server or client) can maintain a single session. The other benefit of a consistent address is that an access list can be configured on the remote device.

The specified interface must have an IP address associated with it. If the specified interface does not have an IP address or is in a down state, then rcp/rsh reverts to the default. To avoid this, add an IP address to the subinterface or bring the interface to the up state.

Examples

In the following example, Loopback interface 0 is assigned an IP address of 220.144.159.200, and the **ip rcmd source-interface** command is used to specify that the source IP address for all rcp/rsh packets will be the IP address assigned to the Loopback0 interface:

```
interface Loopback0
  description Loopback interface
```

```
  ip address 220.144.159.200 255.255.255.255
  no ip directed-broadcast
!
.
.
.
clock timezone GMT 0
ip subnet-zero
no ip source-route
no ip finger
ip rcmd source-interface Loopback0
ip telnet source-interface Loopback0
ip tftp source-interface Loopback0
ip ftp source-interface Loopback0
ip ftp username cisco
ip ftp password shhhhsecret
no ip bootp server
ip domain-name net.galaxy
ip name-server 220.144.159.1
ip name-server 220.144.159.2
ip name-server 219.10.2.1
!
.
.
.
```

Related Commands

Command	Description
ip rcmd remote-host	Creates an entry for the remote user in a local authentication database so that remote users can execute commands on the router using rsh or rcp.

ip telnet source-interface

To specify the IP address of an interface as the source address for Telnet connections, use the **ip telnet source-interface** command in global configuration mode. To reset the source address to the default for each connection, use the **no** form of this command.

ip telnet source-interface *interface*

no ip telnet source-interface

Syntax Description

interface	The interface whose address is to be used as the source for Telnet connections.

Defaults

The address of the closest interface to the destination is the source address.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Use this command to set the IP address of an interface as the source for all Telnet connections.

If the specified interface is not up, the Cisco IOS software selects the address of the interface closest to the destination as the source address.

Examples

The following example forces the IP address for Ethernet interface 1 as the source address for Telnet connections:

```
Router(config)# ip telnet source-interface Ethernet1
```

Related Commands

Command	Description
ip radius source-interface	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.

ip tftp source-interface

To specify the IP address of an interface as the source address for TFTP connections, use the **ip tftp source-interface** command in global configuration mode. To return to the default, use the **no** form of this command.

ip tftp source-interface *interface*

no ip tftp source-interface

Syntax Description

interface	The interface whose address is to be used as the source for TFTP connections.

Defaults

The address of the closest interface to the destination as the source address.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Use this command to set the IP address of an interface as the source for all TFTP connections.

If the specified interface is not up, the Cisco IOS software selects the address of the interface closest to the destination as the source address.

Examples

In the following example, the IP address assigned to Loopback interface 0 will be used as the source address for TFTP connections:

```
Router(config)# ip tftp source-interface Loopback0
```

Related Commands

Command	Description
ip ftp source-interface	Forces outgoing FTP packets to use the IP address of a specified interface as the source address.
ip radius source-interface	Forces outgoing RADIUS packets to use the IP address of a specified interface as the source address.

Note The **ip wccp** {**web-cache** | *service-number*} **group-list** command syntax resembles the **ip wccp** {**web-cache** | *service-number*} **group-listen** command, but these are entirely different commands. Note that the **ip wccp group-listen** command is an interface configuration command, used to configure an interface to listen for multicast notifications from a cache cluster. See the description of the **ip wccp <service> group-listen** command for more information.

kron occurrence

To specify schedule parameters for a Command Scheduler occurrence and enter kron-occurrence configuration mode, use the **kron occurrence** command in global configuration mode. To delete a Command Scheduler occurrence, use the **no** form of this command.

kron occurrence *occurrence-name* [**user** *username*] {**in** [[*numdays***:**]*numhours***:**]*nummin* | **at** *hours***:***min* [[*month*] *day-of-month*] [*day-of-week*]} {**oneshot** | **recurring**}

no kron occurrence *occurrence-name* [**user** *username*] {**in** [[*numdays***:**]*numhours***:**]*nummin* | **at** *hours***:***min* [[*month*] *day-of-month*] [*day-of-week*]} {**oneshot** | **recurring**}

Syntax Description

occurrence-name	Name of occurrence. Length of *occurrence-name* is from 1 to 31 characters. If the *occurrence-name* is new, an occurrence structure will be created. If the *occurrence-name* is not new, the existing occurrence will be edited.
user	(Optional) Used to identify a particular user.
username	(Optional) Name of user.
in	Identifies that the occurrence is to run after a specified time interval. The timer starts when the occurrence is configured.
*numdays***:**	(Optional) Number of days. If used, add a colon after the number.
*numhours***:**	(Optional) Number of hours. If used, add a colon after the number.
nummin	Number of minutes.
at	Identifies that the occurrence is to run at a specified calendar date and time.
*hours***:**	Hour as a number using the twenty-four hour clock. Add a colon after the number.
min	Minute as a number.
month	(Optional) Month name. If used, you must also specify *day-of-month*.
day-of-month	(Optional) Day of month as a number.
day-of-week	(Optional) Day of week name.
oneshot	Identifies that the occurrence is to run only one time. After the occurrence has run, the configuration is removed.
recurring	Identifies that the occurrence is to run on a recurring basis.

Defaults

No schedule parameters are specified.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use the **kron occurrence** and **policy-list** commands to schedule one or more policy lists to run at the same time or interval. Use the **kron policy-list** command in conjunction with the **cli** command to create a Command Scheduler policy containing EXEC command line interface (CLI) commands to be scheduled to run on the router at a specified time.

Use the **show kron schedule** command to display the name of each configured occurrence and when it will next run.

The Command Scheduler process is useful to automate the running of EXEC commands at recurring intervals, and it can be used in remote routers to minimize manual intervention.

Examples

The following example shows how to create a Command Scheduler occurrence named IT2 and schedule it to run every three days, 10 hours, and 50 minutes. The EXEC CLI in the policy named three-day-list is configured to run as part of occurrence info-three.

```
Router(config)# kron occurrence info-three user IT2 in 3:10:50 recurring
Router(config-kron-occurrence)# policy-list three-day-list
```

The following example shows how to create a Command Scheduler occurrence named auto-mkt and schedule it to run once on June 4 at 5:30 a.m. The EXEC CLI in the policies named mkt-list and mkt-list2 are configured to run as part of occurrence auto-mkt.

```
Router(config)# kron occurrence auto-mkt user marketing at 5:30 jun 4 oneshot
Router(config-kron-occurrence)# policy-list mkt-list
Router(config-kron-occurrence)# policy-list mkt-list2
```

Related Commands

Command	Description
cli	Specifies EXEC CLI commands within a Command Scheduler policy list
kron policy-list	Specifies a name for a Command Scheduler policy and enters kron-policy configuration mode.
policy-list	Specifies the policy list associated with a Command Scheduler occurrence.
show kron schedule	Displays the status and schedule information for Command Scheduler occurrences.

kron policy-list

To specify a name for a Command Scheduler policy and enter kron-policy configuration mode, use the **kron policy-list** command in global configuration mode. To delete the policy list, use the **no** form of this command.

kron policy-list *list-name*

no kron policy-list *list-name*

Syntax Description

list-name	Name of policy. Length of *list-name* is from 1 to 31 characters. If the *list-name* is new, a policy list structure will be created. If the *list-name* is not new, the existing policy list will be edited.

Defaults

If the specified list name does not exist, a new policy list is created.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use the **kron policy-list** command in conjunction with the **cli** command to create a Command Scheduler policy containing EXEC command line interface (CLI) commands to be scheduled to run on the router at a specified time. Use the **kron occurrence** and **policy-list** commands to schedule one or more policy lists to run at the same time or interval.

The Command Scheduler process is useful to automate the running of EXEC commands at recurring intervals, and it can be used in remote routers to minimize manual intervention.

Examples

The following example shows how to create a policy named sales-may and configure EXEC CLI commands to run the CNS command that retrieves an image from a server:

```
Router(config)# kron policy-list sales-may
Router(config-kron-policy)# cli cns image retrieve server https://10.21.2.3/imgsvr/ status
https://10.21.2.5/status/
```

Related Commands

Command	Description
cli	Specifies EXEC CLI commands within a Command Scheduler policy list.
kron occurrence	Specifies schedule parameters for a Command Scheduler occurrence and enters kron-occurrence configuration mode.
policy-list	Specifies the policy list associated with a Command Scheduler occurrence.

length

To set the terminal screen length, use the **length** command in line configuration mode. To restore the default value, use the **no** form of this command.

length *screen-length*

no length

Syntax Description

screen-length	The number of lines on the screen. A value of zero disables pausing between screens of output.

Defaults

Screen length of 24 lines

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The Cisco IOS software uses the value of this command to determine when to pause during multiple-screen output. Not all commands recognize the configured screen length. For example, the **show terminal** command assumes a screen length of 24 lines or more.

Examples

In the following example, the terminal type is specified and the screen pause function is disabled for the terminal connection on line 6:

```
Router(config)# line 6
Router(config-line)# terminal-type VT220
Router(config-line)# length 0
```

Related Commands

Command	Description
terminal length	Sets the number of lines on the current terminal screen for the current session.

line-cli

Note Effective with Cisco IOS Releases 12.3(8)T and 12.3(9), the **line-cli** command is replaced by the **cli (cns)** command. See the **cli (cns)** command for more information.

To connect to the Cisco Networking Services (CNS) configuration engine using a modem dialup line, use the **line-cli** command in CNS Connect-interface configuration mode.

line-cli

Syntax Description

This command has no arguments or keywords.

Defaults

No command lines are specified to configure modem lines.

Command Modes

CNS Connect-interface configuration

Command History

Release	Modification
12.2(8)T	This command was introduced on Cisco 2600 series and Cisco 3600 series routers.
12.3(8)T	This command was replaced by the **cli (cns)** command.
12.3(9)	This command was replaced by the **cli (cns)** command.

Usage Guidelines

Use this command to connect to the CNS configuration engine using a specific type of interface. You must specify the interface type but need not specify the interface number; the router's bootstrap configuration finds the connecting interface, regardless of the slot in which the card resides or the modem dialout line for the connection, by trying different candidate interfaces or lines until it successfully pings the registrar.

Enter this command to enter CNS Connect-interface configuration (config-cns-conn-if) mode. Then use one of the following bootstrap-configuration commands to connect to the registrar for initial configuration:

- **config-cli** followed by commands that, used as is, configure the interface.
- **line-cli** followed by a command to configure modem lines to enable dialout and, after that, commands to configure the modem dialout line.

The **config-cli** command accepts the special directive character "**&**," which acts as a placeholder for the interface name. When the configuration is applied, the **&** is replaced with the interface name. Thus, for example, if we are able to connect using FastEthernet0/0, the following is the case:

- The **config-cli ip route 0.0.0.0 0.0.0.0 &** command generates the **config ip route 0.0.0.0 0.0.0.0 FastEthernet0/0** command.
- The **cns id & ipaddress** command generates the **cns id FastEthernet0/0 ipaddress** command.

Examples

The following example enters CNS Connect-interface configuration mode, connects to a configuration engine using an asynchronous interface, and issues a number of commands:

```
Router(config)# cns config connect-intf Async
Router(config-cns-conn-if)# config-cli encapsulation ppp
Router(config-cns-conn-if)# config-cli ip unnumbered FastEthernet0/0
Router(config-cns-conn-if)# config-cli dialer rotart-group 0
Router(config-cns-conn-if)# line-cli modem InOut
Router(config-cns-conn-if)# line-cli
.
.
.
Router(config-cns-conn-if)# exit
```

These commands apply the following configuration:

```
line 65
modem InOut
.
.
.
interface Async65
encapsulation ppp
dialer in-band
dialer rotary-group 0
```

Related Commands

Command	Description
cns config connect-intf	Specifies the interface for connecting to the CNS configuration engine.
config-cli	Connects to the CNS configuration engine using a specific type of interface.

lives-of-history-kept

To set the number of lives maintained in the history table for the Service Assurance Agent (SAA) operation, use the **lives-of-history-kept** command in SAA RTR configuration mode. To return to the default value, use the **no** form of this command.

lives-of-history-kept *lives*

no lives-of-history-kept

Syntax Description

lives	Number of lives maintained in the history table for the operation. If you specify **0** lives, history is not collected for the operation.

Defaults

0 lives

Command Modes

SAA RTR configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The number of lives you can specify is dependent on the type of operation you are configuring. Use the **lives-of-history-kept ?** command to determine the available options.

The default value of 0 lives means that history is not collected for the operation.

To disable history collection, use **no lives-of-history-kept** command rather than the **filter-for-history none** SAA RTR configuration command. The **no lives-of-history-kept** command disables history collection before an operation is attempted, while the **filter-for-history** command causes the SAA to check for history inclusion after the operation attempt is made.

When the number of lives exceeds the specified value, the history table wraps (that is, the oldest information is replaced by newer information).

When an operation makes a transition from pending to active, a life starts. When the life of an operation ends, the operation makes a transition from active to pending.

Examples

The following example maintains the history for 5 lives of operation 1:

```
Router(config)# rtr 1
Router(config-rtr)# type echo protocol ipIcmpEcho 172.16.1.176
Router(config-rtr)# lives-of-history-kept 5
```

Related Commands

Command	Description
buckets-of-history-kept	Sets the number of history buckets that are kept during the lifetime of the SAA.
filter-for-history	Defines the type of information kept in the history table for the SAA operation.
rtr	Enters SAA RTR configuration mode.
samples-of-history-kept	Sets the number of entries kept in the history table per bucket for the SA Agent operation.

load-interval

To specify the length of time to be used to calculate the average load for an interface, use the **load-interval** command in interface configuration or Frame Relay DLCI configuration mode. To revert to the default setting, use the **no** form of this command.

load-interval *seconds*

no load-interval *seconds*

Syntax Description

seconds	Length of time for which data is used to compute load statistics. Value is a multiple of 30, from 30 to 600 (30, 60, 90, 120, and so on). The default is 300 seconds.

Defaults

300 seconds (5 minutes)

Command Modes

Interface configuration
Frame Relay DLCI configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(4)T	This command was made available in Frame Relay DLCI configuration mode.

Usage Guidelines

If you want load computations to be more reactive to short bursts of traffic, rather than being averaged over 5-minute periods, you can shorten the length of time over which load averages are computed. For example, if the load interval is set to 30 seconds, the load value will reflect the weighted-average load for the last 30-second period.

Load data is gathered every 5 seconds. This data is used to compute load statistics, including input rate in bits and packets per second, output rate in bits and packets per second, load, and reliability. Load data is computed using a weighted-average calculation in which recent load data has more weight in the computation than older load data.

The **load-interval** command allows you to change the calculation interval from the default value of 5 minutes (300 seconds) to a shorter or longer period of time. If you change it to a shorter period of time, the input and output statistics that are displayed when you use the **show interface** or **show frame-relay pvc** command will be more current, rather than reflecting a more average load over a longer period of time.

One use of this command is to increase or decrease the likelihood of activating a backup interface; for example a backup dial interface may be triggered by a sudden spike in the load on an active interface.

Examples

In the following example, the load-interval for the serial interface 0 is configured so that the average is computed over 30-second intervals. A burst in traffic that would not trigger a dial backup for an interface configured with the default 5-minute interval might trigger a dial backup for this interface, which is set for the shorter 30-second interval.

```
Router(config)# interface serial 0
Router(config-if)# load-interval 30
```

Frame Relay PVC Example

In the following example, the load interval is set to 60 seconds for a Frame Relay PVC with the DLCI 100:

```
Router(config)# interface serial 1/1
Router(config-if# encapsulation frame-relay ietf
Router(config-if)# frame-relay interface-dlci 100
Router(config-fr-dlci)# load-interval 60
```

Related Commands

Command	Description
show interfaces	Displays information about interfaces on the device.

location

To provide a description of the location of a serial device, use the **location** command in line configuration mode. To remove the description, use the **no** form of this command.

location *text*

no location

Syntax Description

text	Location description.

Defaults

No location description is provided.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **location** command enters information about the device location and status. Use the **show users all** EXEC command to display the location information.

Examples

In the following example, the location description for the console line is given as "Building 3, Basement":

```
Router(config)# line console
Router(config-line)# location Building 3, Basement
```

lock

To configure a temporary password on a line, use the **lock** command in EXEC mode.

lock

Syntax Description

This command has no arguments or keywords.

Defaults

Not locked

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced in a release prior to Cisco IOS Release 10.0.

Usage Guidelines

You can prevent access to your session while keeping your connection open by setting up a temporary password. To lock access to the terminal, perform the following steps:

Step 1 Enter the **lock** command. The system prompts you for a password.

Step 2 Enter a password, which can be any arbitrary string. The system will prompt you to confirm the password. The screen then clears and displays the message "Locked."

Step 3 To regain access to your sessions, reenter the password.

The Cisco IOS software honors session timeouts on a locked lines. You must clear the line to remove this feature. The system administrator must set the line up to allow use of the temporary locking feature by using the **lockable** line configuration command.

Examples

The following example shows configuring the router as lockable, saving the configuration, and then locking the current session for the user:

```
Router(config-line)# lockable
Router(config-line)# ^Z
Router# copy system:running-config nvram:startup-config
Building configuration...
OK
Router# lock
Password: <password>
Again: <password>
                        Locked
Password: <password>
Router#
```

Related Commands

Command	Description
lockable	Enables the **lock** EXEC command.
login (EXEC)	Enables or changes a login username.

lockable

To enable use of the **lock** EXEC command, use the **lockable** command in line configuration mode. To reinstate the default (the terminal session cannot be locked), use the **no** form of this command.

lockable

no lockable

Syntax Description

This command has no arguments or keywords.

Defaults

Sessions on the line are not lockable (the **lock** EXEC command has no effect).

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command enables use of temporary terminal locking, which is executed using the **lock** EXEC command. Terminal locking allows a user keep the current session open while preventing access by other users.

Examples

In the following example, the terminal connection is configured as lockable, then the current connection is locked:

```
Router# configure terminal
Router(config)# line console 0
Router(config-line)# lockable
Router(config)# ^Z
Router# lock
Password: <password>
Again: <password>
                      Locked

Password: <password>
Router#
```

Related Commands

Command	Description
lock	Prevents access to your session by other users by setting a temporary password on your terminal line.

logging buffered

To enable system message logging to a local buffer and limit messages logged to the buffer based on severity, use the **logging buffered** command in global configuration mode. To cancel the use of the buffer, use the **no** form of this command. The **default** form of this command returns the buffer size to the default size.

logging buffered [*buffer-size* | *level*]

no logging buffered

default logging buffered

Syntax Description

buffer-size	(Optional) Size of the buffer from 4096 to 4,294,967,295 bytes. The default size varies by platform.
level	(Optional) Limits the logging of messages to the buffer to a specified level. You can enter the level name or level number. See Table 27 for a list of the accepatable level name or level number keywords. The default logging level varies by platform, but is generally 7, meaning that messages at all levels (0-7) are logged to the buffer.

Defaults

Varies by platform. For most platforms, logging to the buffer is disabled by default. When enabled, the default logging level is 7 (debugging).

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.1(17)T	The *level* argument was added.

Usage Guidelines

This command copies logging messages to an internal buffer. The buffer is circular in nature, so newer messages overwrite older messages after the buffer is filled.

Specifying a *level* causes messages at that level and numerically lower levels to be logged in an internal buffer. See Table 27 for a list of level arguments.

Do not make the buffer size too large because the router could run out of memory for other tasks. You can use the **show memory** EXEC command to view the free processor memory on the router; however, this is the maximum available and should not be approached. The **default logging buffered** command resets the buffer size to the default for the platform.

To display the messages that are logged in the buffer, use the **show logging** command. The first message displayed is the oldest message in the buffer.

The **show logging** command displays the addresses and levels associated with the current logging setup, and any other logging statistics.

Table 27 Error Message Logging Priorities and Corresponding Level Names/Numbers

Level Name	Level Number	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Examples

In the following example, the user enables standard system logging to the local syslog buffer:

```
Router(config)# logging buffered
```

Related Commands

Command	Description
clear logging	Clears messages from the logging buffer.
logging buffered xml	Enables system message logging (syslog) and sends XML-formatted logging messages to the XML-specific system buffer.
show logging	Displays the state of logging (syslog).

logging buffered xml

To enable system message logging (syslog) and send XML-formatted logging messages to the XML-specific system buffer, use the **logging buffered xml** command in global configuration mode. To disable the XML syslog buffer and return the size of the buffer to the default, use the **no** form of this command.

logging buffered xml [*xml-buffer-size*]

no logging buffered xml

Syntax Description

xml-buffer-size	(Optional) Size of the buffer, from 4,096 to 4,294,967,295 bytes (4 kilobytes to 2 gigabytes). The default size varies by platform. This value is ignored if entered as part of the **no** form of this command.

Defaults

XML formatting of system logging messages is disabled.

The default XML syslog buffer size is the same size as the standard syslog buffer.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Standard logging is enabled by default, but XML-formatted system message logging is disabled by default. If standard logging has been disabled on your system (using the **no logging on** command), standard logging must be reenabled using the **logging on** command before using the **logging buffered xml** command.

The **logging buffered xml** command copies logging messages to an internal XML buffer. The XML syslog buffer is separate from the standard syslog buffer (created using the **logging buffered** command).

The buffer is circular, so newer messages overwrite older messages as the buffer is filled.

The severity level for logged messages is determined by the setting of the **logging buffered** command. If the **logging buffered** command has not been used, the default severity level for that command is used. The default severity level varies by platform, but is generally level 7 (“debugging”), meaning that messages at all severity levels (0 through 7) are logged. For more information on severity levels, see the documentation of the **logging buffered** command.

Do not make the buffer size too large because the router could run out of memory for other tasks. You can use the **show memory** EXEC command to view the free processor memory on the router; however, this value is the maximum available and should not be approached.

To return the size of the XML logging buffer to the default, enter the **logging buffered xml** command again without a buffer size value.

To display the messages that are logged in the buffer, use the **show logging xml** command in EXEC mode. The first message displayed is the oldest message in the buffer.

Examples

In the following example, the user enables logging to the XML syslog buffer and sets the XML syslog buffer size to 14 kilobytes:

```
Router(config)# logging buffered xml 14336
```

Related Commands

Command	Description
clear logging xml	Clears all messages from the XML-specific system message logging (syslog) buffer.
logging buffered	Enables standard system message logging (syslog) to a local buffer and sets the severity level and buffer size for the logging buffer.
logging on	Globally controls (enables or disables) system message logging.
show logging xml	Displays the state of XML-formatted system message logging, followed by the contents of the XML-specific buffer.

logging console

To send system logging (syslog) messages to all available TTY lines and limit messages based on severity, use the **logging console** command in global configuration mode. To disable logging to the console terminal, use the **no** form of this command.

logging console [*severity-level*]

no logging console [*severity-level*]

Syntax Description

severity-level	Limits the logging of messages displayed on the console terminal to the specified level and (numerically) lower levels. You can enter the level number or level name. See Table 28 for a list of the level arguments.

Defaults

In general, the default is to log messages from level 0 (emergencies) to level 7 (debugging). However, the default level varies by platform.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **console** keyword indicates all available TTY lines. This can mean a console terminal attached to the router's TTY line, a dial-up modem connection, or a printer.

Specifying a level causes messages at that level and numerically lower levels to be sent to the console (TTY lines). See Table 28 for a list of the level arguments.

The **show logging** EXEC command displays the addresses and levels associated with the current logging setup, and any other logging statistics.

Table 28 Error Message Logging Priorities and Corresponding Level Names/Numbers

Level Arguments	Level	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Note The effect of the **log** keyword with the IP **access list (extended)** interface configuration command depends on the setting of the **logging console** command. The **log** keyword takes effect only if the logging console level is set to 6 or 7. If you change the default to a level lower than 6 and specify the **log** keyword with the IP **access list (extended)** command, no information is logged or displayed.

Examples

In the following example, the user changes the level of messages sent to the console terminal (TTY lines) to **alerts**, which means messages at levels 0 and 1 are sent:

```
Router(config)# logging console alerts
```

Related Commands

Command	Description
access-list (extended)	Defines an extended XNS access list.
logging facility	Configures the syslog facility in which error messages are sent.

logging console xml

To enable XML-formatted system message logging to the console connections, use the **logging console xml** command in global configuration mode. To disable all logging to the console connections, use the **no** form of this command.

logging console xml [*severity-level*]

no logging console xml

Syntax Description

severity-level	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): {**0** | **emergencies**}— System is unusable {**1** | **alerts**}—Immediate action needed {**2** | **critical**}—Critical conditions {**3** | **errors**}—Error conditions {**4** | **warnings**}—Warning conditions {**5** | **notifications**}—Normal but significant conditions {**6** | **informational**}—Informational messages {**7** | **debugging**}— Debugging messages

Defaults

Logging to the console is enabled.

XML-formatted logging to the console is disabled.

The default severity level varies by platform, but is generally level 7 (messages at levels 0 through 7 are logged).

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

To return system logging messages to standard text (without XML formatting), issue the standard **logging console** command (without the **xml** keyword extension).

Examples

In the following example, the user enables XML-formatted system message logging to the console for messages at levels 0 through 4:

```
Router(config)# logging console xml 4
```

Related Commands

Command	Description
show logging xml	Displays the state of XML-formatted system message logging, followed by the contents of the XML syslog buffer.

logging count

To enable the error log count capability, use the **logging count** command in global configuration mode. To disable the error log count capability, use the **no** form of this command.

logging count

no logging count

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

The **logging count** command counts every syslog message and time-stamps the occurrence of each message.

Examples

In the following example, syslog messages are logged to the system buffer and the logging count capability is enabled:

```
Router(config)# logging buffered notifications
Router(config)# logging count
Router(config)# end
Router# show logging count

Facility       Message Name                    Sev Occur   Last Time

================================================================================
SYS            BOOTTIME                         6    1     00:00:12
SYS            RESTART                          5    1     00:00:11
SYS            CONFIG_I                         5    3     1d00h
-------------  -------------------------------  -----------------------------
SYS TOTAL                                           5

LINEPROTO      UPDOWN                           5   13 00:00:19
-------------  -------------------------------  -----------------------------
LINEPROTO TOTAL                                    13

LINK           UPDOWN                           3    1 00:00:18
LINK           CHANGED                          5   12 00:00:09
-------------  -------------------------------  -----------------------------
```

```
LINK TOTAL                                          13

SNMP           COLDSTART                          5    1 00:00:11
-------------  -------------------------------  ----------------------------
SNMP TOTAL
```

Related Commands

Command	Description
show logging	Displays the state of system logging (syslog).

logging cns-events

To enable XML-formatted system event message logging to be sent trough the CNS Event Bus, use the **logging cns-events** command in global configuration mode. To disable the ability to send system logging event messages through the CNS Event Bus, use the **no** form of this command.

logging cns-events [*severity-level*]

no logging cns-events

Syntax Description

severity-level	The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): {**0** | **emergencies**}— System is unusable {**1** | **alerts**}—Immediate action needed {**2** | **critical**}—Critical conditions {**3** | **errors**}—Error conditions {**4** | **warnings**}—Warning conditions {**5** | **notifications**}—Normal but significant conditions {**6** | **informational**}—Informational messages {**7** | **debugging**}— Debugging messages

Defaults

Level 7: debugging

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

Before you configure this command you must enable the CNS event agent with the **cns event** command because the CNS event agent sends out the CNS event logging messages. The generation of many CNS event logging messages can negatively impact the publishing time of standard CNS event messages that must be sent to the network.

If the **debug cns event** command is active when the **logging cns-events** command is configured, the logging of CNS events is disabled.

Examples

In the following example, the user enables XML-formatted CNS system error message logging to the CNS Event Bus for messages at levels 0 through 4:

```
Router(config)# logging cns-events 4
```

Related Commands

Command	Description
cns event	Configures CNS event gateway, which provides CNS event services to Cisco IOS clients.
debug cns event	Displays CNS event agent debugging messages.

logging facility

To configure the syslog facility in which error messages are sent, use the **logging facility** command in global configuration mode. To revert to the default of **local7**, use the **no** form of this command.

logging facility *facility-type*

no logging facility

Syntax Description

facility-type	Syslog facility. See the "Usage Guidelines" section of this command reference entry for descriptions of acceptable keywords.

Defaults

local7

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Table 29 describes the acceptable keywords for the *facility-type* argument.

Table 29 logging facility facility-type Argument

Facility-type keyword	Description
auth	Authorization system
cron	Cron facility
daemon	System daemon
kern	Kernel
local0–7	Reserved for locally defined messages
lpr	Line printer system
mail	Mail system
news	USENET news
sys9	System use
sys10	System use
sys11	System use
sys12	System use
sys13	System use
sys14	System use
syslog	System log

Table 29 logging facility facility-type Argument (continued)

Facility-type keyword	Description
user	User process
uucp	UNIX-to-UNIX copy system

Examples

In the following example, the user configures the syslog facility to the kernel facility type:

```
logging facility kern
```

Related Commands

Command	Description
logging console	Limits messages logged to the console based on severity.

logging history

To limit syslog messages sent to the router's history table and to an SNMP network management station based on severity, use the **logging history** command in global configuration mode. To return the logging of syslog messages to the default level, use the **no** form of this command with the previously configured severity level argument.

logging history [*severity-level-name* | *severity-level-number*]

no logging history [*severity-level-name* | *severity-level-number*]

Syntax Description

severity-level-name	Name of the severity level. Specifies the lowest severity level for system error message logging. See the "Usage Guidelines" section of this command for available keywords.
severity-level-number	Number of the severity level. Specifies the lowest severity level for system error message logging. See the "Usage Guidelines" section of this command for available keywords.

Defaults

Logging of error messages of severity levels 0 through 4 (emergency, alert, critical, error, and warning levels); in other words, "saving level warnings or higher."

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The sending of syslog messages to an SNMP network management station (NMS) occurs when you enable syslog traps with the **snmp-server enable traps syslog** global configuration mode command.

Because SNMP traps are potentially unreliable, at least one syslog message, the most recent message, is stored in a history table on the router. The history table, which contains table size, message status, and message text data, can be viewed using the **show logging history** command. The number of messages stored in the table is governed by the **logging history size** global configuration mode command.

Severity levels are numbered 0 through 7, with 0 being the highest severity level and 7 being the lowest severity level (that is, the lower the number, the more critical the message). Specifying a *level* causes messages at that severity level and numerically lower levels to be stored in the router's history table and sent to the SNMP network management station. For example, specifying the level **critical** causes messages as the critical (3), alert (2), and emergency (1) levles to be saved to the logging history table.

Table 30 provides a description of logging severity levels, listed from higest severity to lowest severity, and the arguments used in the **logging history** command syntax. Note that you can use the level name or the level number as the *level* argument in this command.

Table 30 Syslog Error Message Severity Levels

Severity Level Name	Severity Level Number	Description	Syslog Definition
emergencies	**0**	System unusable	LOG_EMERG
alerts	**1**	Immediate action needed	LOG_ALERT
critical	**2**	Critical conditions	LOG_CRIT
errors	**3**	Error conditions	LOG_ERR
warnings	**4**	Warning conditions	LOG_WARNING
notifications	**5**	Normal but significant condition	LOG_NOTICE
informational	**6**	Informational messages only	LOG_INFO
debugging	**7**	Debugging messages	LOG_DEBUG

Examples

In the following example, the system is initially configured to the default of saving severity level 4 or higher. The **logging history 1** command is used to configure the system to save only level 1 (alert) and level 0 (emergency) messages to the logging history table, and, by extension, to send only these levels in the SNMP notifications. The configuration is then confirmed using the **show logging history** command.

```
Router# show logging history
Syslog History Table:10 maximum table entries,
! The following line shows that system-error-message-logging is set to the
! default level of "warnings" (4).
saving level warnings or higher
 23 messages ignored, 0 dropped, 0 recursion drops
 1 table entries flushed
 SNMP notifications not enabled
   entry number 2 : LINK-3-UPDOWN
    Interface FastEthernet0, changed state to up
    timestamp: 2766
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# logging history 1
Router(config)# snmp-server enable traps syslog
Router(config)# end
Router#
4w0d: %SYS-5-CONFIG_I: Configured from console by console
Router# show logging history
Syslog History Table:1 maximum table entries,
! The following line indicates that 'logging history level 1' (alerts) is configured.
saving level alerts or higher
 18 messages ignored, 0 dropped, 0 recursion drops
 1 table entries flushed
 SNMP notifications enabled, 0 notifications sent
   entry number 2 : LINK-3-UPDOWN
    Interface FastEthernet0, changed state to up
    timestamp: 2766
Router#
```

Related Commands

Command	Description
logging history size	Sets the maximum number of syslog messages that can be stored in the router's syslog history table.
logging on	Controls (enables or disables) the logging of error messages.
show logging	Displays the state of system logging (syslog) and contents of the local logging buffer.
show logging history	Displays information about the system logging history table.
snmp-server enable traps syslog	Controls (enables or disables) the sending of SYSLOG MIB notifications.
snmp-server host	Specifies the recipient of an SNMP notification operation.

logging history size

To change the number of syslog messages stored in the router's history table, use the **logging history size** command in global configuration mode. To return the number of messages to the default value, use the **no** form of this command.

logging history size *number*

no logging history size

Syntax Description

number	Number from 1 to 500 that indicates the maximum number of messages stored in the history table. The default is one message.

Defaults

One message

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

When the history table is full (that is, it contains the maximum number of message entries specified with the **logging history size** command), the oldest message entry is deleted from the table to allow the new message entry to be stored.

Examples

In the following example, the user sets the number of messages stored in the history table to 20:

```
logging history size 20
```

Related Commands

Command	Description
logging history	Limits syslog messages sent to the router's history table and the SNMP network management station based on severity.
show logging	Displays the state of logging (syslog).

logging host

To log system messages and debug output to a remote host, use the **logging host** command in global configuration mode. To remove a specified logging host from the configuration, use the **no** form of this command.

logging host {*ip-address* | *host-name*} [**xml**]

no logging host {*ip-address* | *host-name*} [**xml**]

Syntax Description

ip-address	IP address of the host to be used as a syslog server.
host-name	Name of the host to be used as a syslog server.
xml	(Optional) Specifies that the logging output should be tagged using the Cisco defined XML tags. This applies to system logging messages only (not to debug command output).

Defaults

System logging messages are not sent to any remote host.

If this command is entered without the **xml** keyword, messages are sent in the standard format.

Command Modes

Global configuration

Command History

Release	Modification
10.0	The **logging** command was introduced.
12.0(14)S, 12.0(14)ST, 12.2(15)T	The **logging host** command replaced the **logging** command.
12.2(15)T	The **xml** keyword was added.

Usage Guidelines

System logging messages are also called system error messages.

Standard system message logging (syslog) is enabled by default. If logging has been disabled on your system (using the **no logging on** command), logging must be reenabled using the **logging on** command before using the **logging host** command.

The **logging host** command identifies a remote host (syslog server) to receive logging messages. By issuing this command more than once, you build a list of syslog servers that receive logging messages.

To specify the severity level for logging to all hosts, use the **logging trap** command.

You can specify that standard syslog messages are to be sent to one or more hosts while XML-formatted messages are to be sent to another host (or hosts) by repeating this command with the appropriate syntax.

If you enter the **logging host** {*ip-address* | *host-name*} command after entering the **logging host** {*ip-address* | *host-name*} **xml** command and you use the same IP adderess or host name in both commands, XML formatting is disabled for that host, and messages will be sent in the standard format. In other words, a standard **logging host** command will replace an XML **logging host** command, and vice versa, if the same host is specified.

Note Any **no logging host** command (with or without the **xml** keyword) will disable all logging to the specified host.

Examples

In the following example, messages at severity levels 0 (emergencies) through 5 (notifications) are logged to a host at 209.165.202.169:

```
Router(config)# logging host 209.165.202.169
Router(config)# logging trap 5
```

Related Commands

Command	Description
logging on	Globally controls (enables or disables) system message logging.
logging trap	Limits messages sent to the syslog servers based on severity level.
show logging	Displays the state of system message logging, followed by the contents of the standard syslog buffer.
show logging xml	Displays the state of XML-formatted system message logging, followed by the contents of the XML syslog buffer.

logging linecard

To log messages to an internal buffer on a line card, use the **logging linecard** command in global configuration mode. To cancel the use of the internal buffer on the line cards, use the **no** form of this command.

logging linecard [*size* | *level*]

no logging linecard

Syntax Description

size	(Optional) Size of the buffer used for each line card. The range is from 4096 to 65,536 bytes. The default is 8 KB.
level	(Optional) Limits the logging of messages displayed on the console terminal to a specified level. The message level can be one of the following: • **alerts**—Immediate action needed • **critical**—Critical conditions • **debugging**—Debugging messages • **emergencies**—System is unusable • **errors**—Error conditions • **informational**—Informational messages • **notifications**—Normal but significant conditions • **warnings**—Warning conditions

Defaults

The Cisco IOS software logs messages to the internal buffer on the GRP card.

Command Modes

Global configuration

Command History

Release	Modification
11.2 GS	This command was added to support the Cisco 12000 series Gigabit Switch Routers.

Usage Guidelines

Specifying a message level causes messages at that level and numerically lower levels to be stored in the internal buffer on the line cards.

Table 31 lists the message levels and associated numerical level. For example, if you specify a message level of critical, all critical, alert, and emergency messages will be logged.

Table 31 Message Levels

Level Keyword	Level
emergencies	0
alerts	1
critical	2
errors	3
warnings	4
notifications	5
informational	6
debugging	7

To display the messages that are logged in the buffer, use the **show logging slot** EXEC command. The first message displayed is the oldest message in the buffer.

Do not make the buffer size too large because the router could run out of memory for other tasks. You can use the **show memory** EXEC command to view the free processor memory on the router; however, this is the maximum available and should not be approached.

Examples

The following example enables logging to an internal buffer on the line cards using the default buffer size and logging warning, error, critical, alert, and emergency messages:

```
Router(config)# logging linecard warnings
```

Related Commands

Command	Description
clear logging	Clears messages from the logging buffer.
show logging	Displays the state of logging (syslog).

logging monitor

To enable system message logging to the terminal lines (monitor connections) and limit these messages based on severity, use the **logging monitor** command in global configuration mode. To disable logging to terminal lines other than the console line, use the **no** form of this command.

logging monitor *severity-level*

no logging monitor

Syntax Description

severity-level	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): {**0** | **emergencies**}— System is unusable {**1** | **alerts**}—Immediate action needed {**2** | **critical**}—Critical conditions {**3** | **errors**}—Error conditions {**4** | **warnings**}—Warning conditions {**5** | **notifications**}—Normal but significant conditions {**6** | **informational**}—Informational messages {**7** | **debugging**}— Debugging messages

Defaults

debugging (severity-level 7)

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Specifying a *severity-level* causes messages only at that level and numerically lower levels to be displayed to the monitor (terminal lines).

Examples

In the following example, the user specifies that only messages of the levels **errors**, **critical**, **alerts**, and **emergencies** be logged to monitor connections:

```
Router(config)# logging monitor 3
```

Related Commands

Command	Description
logging monitor xml	Applies XML formatting to messages logged to the monitor connections.
terminal monitor	Displays **debug** command output and system error messages for the current terminal and session.

logging monitor xml

To enable XML-formatted system message logging to monitor connections, use the **logging console xml** command in global configuration mode. To disable all logging to the monitor connections, use the **no** form of this command.

logging monitor xml [*severity-level*]

no logging monitor xml

Syntax Description

severity-level	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): {**0** | **emergencies**}— System is unusable {**1** | **alerts**}—Immediate action needed {**2** | **critical**}—Critical conditions {**3** | **errors**}—Error conditions {**4** | **warnings**}—Warning conditions {**5** | **notifications**}—Normal but significant conditions {**6** | **informational**}—Informational messages {**7** | **debugging**}— Debugging messages

Defaults

Logging to monitor connections is enabled.

XML-formatted logging to monitor connections is disabled.

The default severity level varies by platform, but is generally level 7 (messages at levels 0 through 7 are logged).

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

The **monitor** keyword specifies the tty line connections at all line ports. The tty lines (also called ports) communicate with peripheral devices such as terminals, modems, and serial printers. An example of a tty connection is a PC with a terminal emulation program connected to the device using a dial-up modem, or a Telnet connection.

To return system logging messages to standard text (without XML formatting), issue the standard **logging monitor** command (without the **xml** keyword extension).

Examples

In the following example, the user enables XML-formatted system message logging to the console for messages at levels 0 through 4 and XML-formatted system message logging to tty line connections at the default severity level:

```
Router(config)# logging console xml 4
Router(config)# logging monitor xml
```

Related Commands

Command	Description
logging monitor	Enables system message logging in standard (plain text) format to all monitor (TTY) connections.
show logging xml	Displays the state of XML-formatted system message logging, followed by the contents of the XML syslog buffer.

logging on

To enable logging of system messages, use the **logging on** command in global configuration mode. This command sends debug or error messages to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages. To disable the logging process, use the **no** form of this command.

logging on

no logging on

Syntax Description

This command has no arguments or keywords.

Defaults

The Cisco IOS software sends messages to the asynchronous logging process.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, terminal lines, or syslog server. System logging messages are also known as system error messages. You can turn logging on and off for these destinations individually using the **logging buffered**, **logging monitor**, and **logging** global configuration commands. However, if the **logging on** command is disabled, no messages will be sent to these destinations. Only the console will receive messages.

Additionally, the logging process logs messages to the console and the various destinations after the processes that generated them have completed. When the logging process is disabled, messages are displayed on the console as soon as they are produced, often appearing in the middle of command output.

Caution Disabling the **logging on** command may substantially slow down the router. Any process generating debug or error messages will wait until the messages have been displayed on the console before continuing.

The **logging synchronous** line configuration command also affects the displaying of messages to the console. When the **logging synchronous** command is enabled, messages will appear only after the user types a carriage return.

Examples

The following example shows command output and message output when logging is enabled. The ping process finishes before any of the logging information is printed to the console (or any other destination).

```
Router(config)# logging on
Router(config)# end
```

```
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router# ping dirt

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.129, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
Router#
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sending
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sending
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sending
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sending
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sending
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
```

In the following example, logging is disabled. The message output is displayed as messages are generated, causing the debug messages to be interspersed with the message "Type escape sequence to abort."

```
Router(config)# no logging on
Router(config)# end

%SYS-5-CONFIG_I: Configured from console by console
Router#
Router# ping dirt

IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sendingTyp
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1e
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sending esc
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sendingape
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sendingse
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sendingquen
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1ce to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.129, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 152/152/156 ms
Router#
```

Related Commands

Command	Description
logging host	Logs messages to a syslog server host.
logging buffered	Logs messages to an internal buffer.
logging console	Logs messages to console connections.
logging monitor	Limits messages logged to the terminal lines (monitors) based on severity.
logging synchronous	Synchronizes unsolicited messages and debug output with solicited Cisco IOS software output and prompts for a specific console port line, auxiliary port line, or vty.

logging origin-id

To add an origin identifier to system logging messages sent to remote hosts, use the **logging origin-id** command in global configuration mode. To disable the origin identifier, use the **no** form of this command.

logging origin-id {**hostname** | **ip** | **string** *user-defined-id*}

no logging origin-id {**hostname** | **ip** | **string** *user-defined-id*}

Syntax Description

hostname	Specifies that the hostname will be used as the message origin identifier.
ip	Specifies that the IP address of the sending interface will be used as the message origin identifier.
string *user-defined-id*	Allows you to enter your own identifying description. The *user-defined-id* argument is a string you specify. • You can enter a string with no spaces or use delimiting quotation marks to enclose a string with spaces.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(15)B	This command was integrated into Release 12.2B.
12.3(1) Mainline	The **string** *user-defined-id* syntax was added.
12.2(16)B	The **string** *user-defined-id* syntax was added for Release 12.2B.

Usage Guidelines

The origin identifier is added to the beginning of all system logging (syslog) messages sent to remote hosts. The identifier can be the hostname, the IP address, or any text that you specify. The origin identifier is not added to messages sent to local destinations (the console, monitor, or buffer).

The origin identifier is useful for identifying the source of system logging messages in cases where you send syslog output from multiple devices to a single syslog host.

When specifying your own identification string using the **logging origin-id string** *user-defined-id* command, the system expects a string without spaces. For example:

```
Router(config)# logging origin-id string Cisco_Systems
```

To uses spaces (multiple words) or additional syntax, enclose the string with quotes. For example:

```
Router(config)# logging origin-id string "Cisco Systems, Inc."
```

Examples

In the following example, the origin identifier "Domain 1, router B" will be added to the beginning of all system logging messages sent to remote hosts:

```
Router(config)# logging origin-id string "Domain 1, router B"
```

In the following example, all logging message sent to remote hosts will have the IP address configured for the Serial 1 interface added to the beginning of the message:

```
Router(config)# logging host 209.165.200.225
Router(config)# logging trap 5
Router(config)# logging source-interface serial 1
Router(config)# logging origin-id ip
```

Related Commands

Command	Description
logging host	Enables system message logging to a remote host.
logging source-interface	Forces logging messages to be sent from a specified interface, instead of any available interface.
logging trap	Configures the severity level at or numerically below which logging messages should be sent to a remote host.

logging rate-limit

To limit the rate of messages logged per second, use the **logging rate-limit** command in global configuration mode. To disable the limit, use the **no** form of this command.

logging rate-limit {*number* | **all** | **console**} [**except** *severity*]

no logging rate-limit

Syntax Description

number	Specifies rate of messages logged per second. The valid values are from 1 to 10000.
all	Sets the rate limit to all messages including the debug messages.
console	Sets the rate limit only to console messages.
except	(Optional) Excludes messages of this severity or higher.
severity	(Optional) Sets the logging severity level. The valid levels are from 0 to 7.

Defaults

No limit is set.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

The **logging rate-limit** command controls the output of messages from the system. Use this command if you want to avoid a flood of output messages. You can select the severity of the output messages and output rate by using the **logging rate-limit** command. You can use the **logging rate-limit** command anytime; it will not negatively impact the performance of your system and may improve the system performance by specifying the severities and rates of output messages.

You can use this command with or without the **logging synchronous** line configuration command. For example, if you want to see all severity 0, 1, and 2 messages, use the **no logging synchronous** command and specify **logging rate-limit 10 except 2**. By using the two commands together, you cause all messages of 0, 1, and 2 severity to print and limit the less severe ones (higher than 2) to only 10 per second.

Table 32 compares the error message logging numeric severity level with its equivalent word description.

Table 32 Error Message Logging Severity Level and Equivalent Word Descriptions

Numeric Severity Level	Equivalent Word	Description
0	**emergencies**	System unusable
1	**alerts**	Immediate action needed

Table 32 Error Message Logging Severity Level and Equivalent Word Descriptions

Numeric Severity Level	Equivalent Word	Description
2	**critical**	Critical conditions
3	**errors**	Error conditions
4	**warnings**	Warning conditions
5	**notifications**	Normal but significant condition
6	**informational**	Informational messages only
7	**debugging**	Debugging messages

For additional details about error message logging, see the "Troubleshooting the Router" chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Examples

In the following example, the **logging rate-limit** configuration mode command limits message output to 200 per second:

```
Router(config)# logging rate-limit 200
```

Related Commands

Command	Description
logging synchronous	Synchronizes unsolicited messages and debug output with solicited Cisco IOS software output and prompts for a specific console port line, auxiliary port line, or vty.

logging source-interface

To specify the source IP address of syslog packets, use the **logging source-interface** command in global configuration mode. To remove the source designation, use the **no** form of this command.

logging source-interface *interface-type interface-number*

no logging source-interface

Syntax Description

interface-type	Interface type.
interface-number	Interface number.

Defaults

No interface is specified.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Normally, a syslog message contains the IP address of the interface it uses to leave the router. The **logging source-interface** command specifies that syslog packets contain the IP address of a particular interface, regardless of which interface the packet uses to exit the router.

Examples

In the following example, the user specifies that the IP address for Ethernet interface 0 is the source IP address for all syslog messages:

```
Router(config)# logging source-interface ethernet 0
```

The following example specifies that the IP address for Ethernet interface 2/1 on a Cisco 7000 series router is the source IP address for all syslog messages:

```
Router(config)# logging source-interface ethernet 2/1
```

Related Commands

Command	Description
logging	Logs messages to a syslog server host.

logging synchronous

To synchronize unsolicited messages and debug output with solicited Cisco IOS software output and prompts for a specific console port line, auxiliary port line, or vty, use the **logging synchronous** command in line configuration mode. To disable synchronization of unsolicited messages and debug output, use the **no** form of this command.

logging synchronous [**level** *severity-level* | **all**] [**limit** *number-of-buffers*]

no logging synchronous [**level** *severity-level* | **all**] [**limit** *number-of-buffers*]

Syntax Description

level *severity-level*	(Optional) Specifies the message severity level. Messages with a severity level equal to or higher than this value are printed asynchronously. Low numbers indicate greater severity and high numbers indicate lesser severity. The default value is 2.
all	(Optional) Specifies that all messages are printed asynchronously, regardless of the severity level.
limit *number-of-buffers*	(Optional) Specifies the number of buffers to be queued for the terminal after which new messages are dropped. The default value is 20.

Defaults

This command is disabled.

If you do not specify a severity level, the default value of 2 is assumed.

If you do not specify the maximum number of buffers to be queued, the default value of 20 is assumed.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When synchronous logging of unsolicited messages and debug output is turned on, unsolicited Cisco IOS software output is displayed on the console or printed after solicited Cisco IOS software output is displayed or printed. Unsolicited messages and debug output is displayed on the console after the prompt for user input is returned. To keep unsolicited messages and debug output from being interspersed with solicited software output and prompts. After the unsolicited messages are displayed, the console displays the user prompt again.

When specifying a severity level number, consider that for the logging system, low numbers indicate greater severity and high numbers indicate lesser severity.

When a message queue limit of a terminal line is reached, new messages are dropped from the line, although these messages might be displayed on other lines. If messages are dropped, the notice "%SYS-3-MSGLOST *number-of-messages* due to overflow" follows any messages that are displayed. This notice is displayed only on the terminal that lost the messages. It is not sent to any other lines, any logging servers, or the logging buffer.

Caution By configuring abnormally large message queue limits and setting the terminal to "terminal monitor" on a terminal that is accessible to intruders, you expose yourself to "denial of service" attacks. An intruder could carry out the attack by putting the terminal in synchronous output mode, making a Telnet connection to a remote host, and leaving the connection idle. This could cause large numbers of messages to be generated and queued, and these messages would unlikely consume all available RAM. You should guard against this type of attack through proper configuration.

Examples

In the following example, line 4 is identified and synchronous logging for line 4 is enabled with a severity level of 6. Then another line, line 2, is identified and the synchronous logging for line 2 is enabled with a severity level of 7 and is specified with a maximum number of buffers to be 70,000.

```
Router(config)# line 4
Router(config-line)# logging synchronous level 6
Router(config-line)# exit
Router(config)# line 2
Router(config)# logging synchronous level 7 limit 70000
Router(config-line)# end
Router#
```

Related Commands

Command	Description
line	Identifies a specific line for configuration and starts the line configuration command collection mode.
logging on	Controls logging of error messages and sends debug or error messages to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages.

logging trap

To limit messages logged to remote syslog servers based on severity, use the **logging trap** command in global configuration mode. To return the logging to remote hosts to the default level, use the **no** form of this command.

logging trap *severity-level*

no logging trap

Syntax Description

severity-level	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): {**0** | **emergencies**}— System is unusable {**1** | **alerts**}—Immediate action needed {**2** | **critical**}—Critical conditions {**3** | **errors**}—Error conditions {**4** | **warnings**}—Warning conditions {**5** | **notifications**}—Normal but significant conditions {**6** | **informational**}—Informational messages {**7** | **debugging**}— Debugging messages

Defaults

Syslog messages at level 0 to level 6 are generated, but will only be sent to a remote host if the **logging host** command is configured.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

A trap is an unsolicited message sent to a remote network management host. Logging traps should not be confused with SNMP traps (SNMP logging traps require the use of the CISCO -SYSLOG-MIB, are enabled using the **snmp-server enable traps syslog** command, and are sent using the Simple Network Management Protocol.)

The **show logging** EXEC command displays the addresses and levels associated with the current logging setup. The command output also includes ancillary statistics.

Table 33 lists the syslog definitions that correspond to the system message logging levels. Additionally, four categories of messages are generated by the software, as follows:

- Error messages about software or hardware malfunctions at the LOG_ERR level.
- Output for the debug commands at the LOG_WARNING level.

- Interface up/down transitions and system restarts at the LOG_NOTICE level.
- Reload requests and low process stacks at the LOG_INFO level.

Use the **logging host** and **logging trap** commands to send messages to a remote syslog server.

Table 33 logging trap Error Message Logging Priorities

Level Keyword	Numeric Level Keyword	Description	Syslog Definition
emergencies	**0**	System unusable	LOG_EMERG
alerts	**1**	Immediate action needed	LOG_ALERT
critical	**2**	Critical conditions	LOG_CRIT
errors	**3**	Error conditions	LOG_ERR
warnings	**4**	Warning conditions	LOG_WARNING
notifications	**5**	Normal but significant condition	LOG_NOTICE
informational	**6**	Informational messages only	LOG_INFO
debugging	**7**	Debugging messages	LOG_DEBUG

Examples

In the following example, system messages of levels 0 (emergencies) through 5 (notifications) are sent to the host at 209.165.200.225:

```
Router(config)# logging host 209.165.200.225
Router(config)# logging trap notifications
```

Related Commands

Command	Description
logging host	Enables remote logging of system logging messages and specifies the syslog server host that messages should be sent to.

logout

To close an active terminal session by logging off the router, use the **logout** command in user EXEC mode.

logout

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

User EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

In the following example, the **exit** (global) command is used to move from global configuration mode to privileged EXEC mode, the **disable** command is used to move from privileged EXEC mode to user EXEC mode, and the **logout** command is used to log off (exit from the active session):

```
Router(config)# exit
Router# disable
Router> logout
```

Related Commands

Command	Description
exit (global)	Exits any configuration mode to the next highest mode in the CLI mode hierarchy.

logout-warning

To warn users of an impending forced timeout, use the **logout-warning** command in line configuration mode. To restore the default, use the **no** form of this command.

logout-warning [*seconds*]

logout-warning

Syntax Description

seconds	(Optional) Number of seconds that are counted down before session termination. If no number is specified, the default of 20 seconds is used.

Defaults

No warning is sent to the user.

Command Modes

Line configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This command notifies the user of an impending forced timeout (set using the **absolute-timeout** command).

Examples

In the following example, a logout warning is configured on line 5 with a countdown value of 30 seconds:

```
Router(config)# line 5
Router(config-line)# logout-warning 30
```

Related Commands

Command	Description
absolute-timeout	Sets the interval for closing user connections on a specific line or port.
session-timeout	Sets the interval for closing the connection when there is no input or output traffic.

lsr-path

To define a loose source routing (LSR) path for a Cisco Service Assurance Agent (SAA) IP echo operation, use the **lsr-path** command in SAA RTR configuration mode. To remove the definition, use the **no** form of this command.

lsr-path {*hostname* | *ip-address*} [{*hostname* | *ip-address*} ...]

no lsr-path

Syntax Description

{*hostname* | *ip-address*}	Hostname or IP address of the first hop in the LSR path.
[{*hostname* | *ip-address*}...]	(Optional) Indicates that you can continue specifying host destinations until you specify the final host target. Each host name or IP address specified indicates another hop on the path. The maximum number of hops you can specify is eight. Do not enter the dots (...).

Defaults

LSR path is disabled.

Command Modes

SAA RTR configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

The maximum number of hops available is eight when an LSR path is configured.

Examples

In the following example, the LSR path is defined for SAA echo operation 1. The target destination for the operation is at 172.16.1.176. The first hop on the LSR path is 172.18.4.149. The second hop on the LSR path is 172.18.16.155.

```
Router(config)# rtr 1
Router(config-rtr)# type echo protocol ipIcmpEcho 172.16.1.176
Router(config-rtr)# lsr-path 172.18.4.149 172.18.26.155
```

Related Commands

Command	Description
rtr	Specifies an identification for an SAA operation and enters SAA RTR configuration mode.

memory sanity

To perform a "sanity check" for corruption in buffers and queues, use the **memory sanity** command in global configuration mode. To disable this feature, use the **no** form of this command.

memory sanity [**buffer** | **queue** | **all**]

no memory sanity

Syntax Description

buffer	(Optional) Specifies checking all buffers.
queue	(Optional) Specifies checking all queues.
all	(Optional) Specifies checking all buffers and queues.

Defaults

This command is not enabled by default.
If the **buffer** or **queue** keyword is not specified, a sanity check will be performed on all buffers and queues.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

When the **memory sanity buffer** command is enabled, a sanity check is performed on buffers when a packet buffer is allocated or when a packet buffer is returned to the buffer pool. This command also time-stamps the buffer, which may be useful when tracking the age of a buffer.

The **memory sanity** command can be saved in the startup configuration file and, therefore, it is not necessary to reconfigure this command each time the router is reloaded. Like the **scheduler heapcheck process memory** command, the **memory sanity** command can check for corruption in the I/O memory block.

Enabling the **memory sanity** command may result in slight router performance degradation.

Examples

The following example shows how to perform a sanity check for corruption in all buffers and queues:

```
memory sanity all
```

Related Commands

Command	Description
scheduler heapcheck process memory	Performs a "sanity check" for corruption in memory blocks when a process switch occurs.

memory scan

To enable the Memory Scan feature, use the **memory scan** command in global configuration mode. To restore the router configuration to the default, use the **no** form of this command.

memory scan

no memory scan

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XE	This command was introduced.
12.0(7)T	This command was integrated in Cisco IOS Release 12.0 T for the Cisco 7500 series only.

Usage Guidelines

The Memory Scan feature adds a low-priority background process that searches all installed dynamic random-access memory (DRAM) for possible parity errors. If errors are found in memory areas that are not in use, this feature attempts to scrub (remove) the errors. The time to complete one memory scan and scrub cycle can range from 10 minutes to several hours, depending on the amount of installed memory. The impact of the Memory Scan feature on the central processing unit (CPU) is minimal. To view the status of the memory scan feature on your router, use the **show memory scan** command in EXEC mode.

Examples

The following example enables the Memory Scan feature on a Cisco 7500 series router:

```
Router(config)# memory scan
```

Related Commands

Command	Description
show memory scan	Displays the number and type of parity errors on your system.

memory-size iomem

To reallocate the percentage of DRAM to use for I/O memory and processor memory on Cisco 3600 series routers, use the **memory-size iomem** command in global configuration mode. To revert to the default memory allocation, use the **no** form of this command.

memory-size iomem *i/o-memory-percentage*

no memory-size iomem *i/o-memory-percentage*

Syntax Description

i/o-memory-percentage	The percentage of DRAM allocated to I/O memory. The values permitted are **10**, **15**, **20**, **25**, **30**, **40**, and **50**. A minimum of 4 MB of memory is required for I/O memory.

Defaults

The default memory allocation is 25 percent I/O memory and 75 percent processor memory.

Note If the **smartinit** process has been enabled, the default memory allocation of 25 percent to I/O does not apply. Instead, **smartinit** examines the network modules and then calculates the I/O memory required.

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.

Usage Guidelines

When you specify the percentage of I/O memory in the command line, processor memory automatically acquires the remaining percentage of DRAM memory.

Examples

The following example allocates 40 percent of the DRAM memory to I/O memory and the remaining 60 percent to processor memory:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# memory-size iomem 40
Router(config)# exit
Router# copy system:running-config nvram:startup-config
Building configuration...
[OK]

Router# reload

rommon 1 > boot
program load complete, entry point: 0x80008000, size: 0x32ea24
```

```
Self decompressing the image :
########################################################################################
########################################################################################
############################################################## [OK]
```

menu (EXEC)

To display a preconfigured user menu, use the **menu** command in user EXEC or privileged EXEC mode.

menu *menu-name*

Syntax Description

menu-name	The name of the menu.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

A user menu is a type of user interface where text descriptions of actions to be performed are displayed to the user. The user can use the menu to select services and functions without having to know the details of command-line interface (CLI) commands.

Menus can be created for users in global configuration mode, using the commands listed in the "Related Commands" section.

A menu can be invoked at either the user or privileged EXEC level, but if an item in the menu contains a privileged EXEC command, the user must be logged in at the privileged level for the command to succeed.

Examples

The following example invokes a menu named OnRamp:

```
Router> menu OnRamp

      Welcome to OnRamp Internet Services

       Type a number to select an option;
            Type 9 to exit the menu.

1     Read email

2     UNIX Internet access

3     Resume UNIX connection


6     Resume next connection

9     Exit menu system
```

Related Commands

Command	Description
menu clear-screen	Clears the terminal screen before displaying a menu.
menu command	Specifies underlying commands for user interface menus.
menu default	Specifies the menu item to use as the default.
menu line-mode	Requires the user to press Enter after specifying an option number.
menu options	Sets options for items in user interface menus.
menu prompt	Specifies the prompt for a user interface menu.
menu single-space	Displays menu items single-spaced rather than double-spaced.
menu status-line	Displays a line of status information about the current user at the top of a menu.
menu text	Specifies the text of a menu item in a user interface menu.
menu title	Creates a title, or banner, for a user menu.
no menu	Deletes a specified menu from a menu configuration.

menu clear-screen

To clear the terminal screen before displaying a menu, use the **menu clear-screen** command in global configuration mode.

menu *menu-name* **clear-screen**

Syntax Description

menu-name	Name of the menu this command should be applied to.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command uses a terminal-independent mechanism based on termcap entries defined in the router and the configured terminal type for the user. This command allows the same menu to be used on multiple types of terminals instead of having terminal-specific strings embedded within menu titles. If the termcap entry does not contain a clear string, the menu system enters 24 new lines, causing all existing text to scroll off the top of the terminal screen.

Examples

In the following example, the terminal screen is cleared before displaying the menu named Access1:

```
Router(config)# menu Access1 clear-screen
```

Related Commands

Command	Description
menu (EXEC)	Invokes a user menu.
menu command	Specifies underlying commands for user menus.
menu default	Specifies the menu item to use as the default.
menu line-mode	Requires the user to press Enter after specifying an item.
menu options	Sets options for items in user menus.
menu prompt	Specifies the prompt for a user menu.
menu single-space	Displays menu items single-spaced rather than double-spaced.
menu status-line	Displays a line of status information about the current user at the top of a menu
menu text	Specifies the text of a menu item in a user menu.

Command	Description
menu title	Creates a title, or banner, for a user menu.
no menu	Deletes a specified menu from a menu configuration.

menu command

To specify underlying commands for user menus, use the **menu command** command in global configuration mode.

menu *menu-name* **command** *menu-item* {*command* | **menu-exit**}

Syntax Description

menu-name	Name of the menu. You can specify a maximum of 20 characters.
menu-item	Number, character, or string used as the key for the item. The key is displayed to the left of the menu item text. You can specify a maximum of 18 menu entries. When the tenth item is added to the menu, the line-mode and single-space options are activated automatically.
command	Command to issue when the user selects an item.
menu-exit	Provides a way for menu users to return to a higher-level menu or exit the menu system.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command to assign actions to items in a menu. Use the **menu text** global configuration command to assign text to items. These commands must use the same menu name and menu selection key.

The **menu command** command has a special keyword for the *command* argument, **menu-exit**, that is available only within menus. It is used to exit a submenu and return to the previous menu level, or to exit the menu altogether and return to the EXEC command prompt.

You can create submenus that are opened by selecting entries in another menu. Use the **menu** EXEC command as the *command* for the submenu item.

Note If you nest too many levels of menus, the system prints an error message on the terminal and returns to the previous menu level.

When a menu allows connections (their normal use), the command for an entry activating the connection should contain a **resume** command, or the line should be configured to prevent users from escaping their sessions with the **escape-char none** command. Otherwise, when they escape from a connection and return to the menu, there will be no way to resume the session and it will sit idle until the user logs out.

Specifying the **resume** command as the action that is performed for a selected menu entry permits a user to resume a named connection or connect using the specified name, if there is no active connection by that name. As an option, you can also supply the connect string needed to connect initially. When you do not supply this connect string, the command uses the specified connection name.

You can also use the **resume/next** command, which resumes the next connection in the user's list of connections. This function allows you to create a single menu entry that steps through all of the user's connections.

Note A menu should not contain any exit paths that leave users in an unfamiliar interface environment.

When a particular line should always display a menu, that line can be configured with an **autocommand** line configuration command. Menus can be run on a per-user basis by defining a similar **autocommand** command for that local username. For more information about the **autocommand** command, refer to the *Cisco IOS Dial Technologies Configuration Guide*.

Examples

In the following example, the commands to be issued when the menu user selects option 1, 2, or 3 are specified for the menu named Access1:

```
menu Access1 command 1 tn3270 vms.cisco.com
menu Access1 command 2 rlogin unix.cisco.com
menu Access1 command 3 menu-exit
```

The following example allows a menu user to exit a menu by entering **Exit** at the menu prompt:

```
menu Access1 text Exit Exit
```
menu Access1 command Exit menu-exit

Related Commands

Command	Description
autocommand	Configures the Cisco IOS software to automatically execute a command when a user connects to a particular line.
menu (EXEC)	Invokes a user menu.
menu clear-screen	Clears the terminal screen before displaying a menu.
menu default	Specifies the menu item to use as the default.
menu line-mode	Requires the user to press Enter after specifying an item.
menu options	Sets options for items in user menus.
menu prompt	Specifies the prompt for a user menu.
menu single-space	Displays menu items single-spaced rather than double-spaced.
menu status-line	Displays a line of status information about the current user at the top of a menu
menu text	Specifies the text of a menu item in a user menu.
menu title	Creates a title, or banner, for a user menu.

menu default

To specify the menu item to use as the default, use the **menu default** command in global configuration mode.

menu *menu-name* **default** *menu-item*

Syntax Description

menu-name	Name of the menu. You can specify a maximum of 20 characters.
menu-item	Number, character, or string key of the item to use as the default.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command to specify which menu entry is used when the user presses Enter without specifying an item. The menu entries are defined by the **menu command** and **menu text** global configuration commands.

Examples

In the following example, the menu user exits the menu when pressing Enter without selecting an item:

```
menu Access1 9 text Exit the menu
menu Access1 9 command menu-exit
menu Access1 default 9
```

Related Commands

Command	Description
menu (EXEC)	Invokes a preconfigured user menu.
menu command	Specifies underlying commands for user menus.
menu prompt	Specifies the prompt for a user menu.
menu text	Specifies the text of a menu item in a user menu.
menu title	Creates a title, or banner, for a user menu.

menu line-mode

To require the user to press Enter after specifying an item, use the **menu line-mode** command in global configuration mode.

menu *menu-name* **line-mode**

Syntax Description

menu-name	Name of the menu this command should be applied to.

Defaults

Enabled for menus with more than nine items. Disabled for menus with nine or fewer items.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

In a menu of nine or fewer items, you ordinarily select a menu item by entering the item number. In line mode, you select a menu entry by entering the item number and pressing Enter. Line mode allows you to backspace over the selected number and enter another number before pressing Enter to issue the command.

This option is activated automatically when more than nine menu items are defined but also can be configured explicitly for menus of nine or fewer items.

In order to use strings as keys for items, the **menu line-mode** command must be configured.

Examples

In the following example, the line-mode option is enabled for the menu named Access1:

```
menu Access1 line-mode
```

Related Commands

Command	Description
menu (EXEC)	Invokes a preconfigured user menu.
menu clear-screen	Clears the terminal screen before displaying a menu.
menu command	Specifies underlying commands for a user menu.
menu default	Specifies the menu item to use as the default.
menu options	Sets options for items in user menus.
menu prompt	Specifies the prompt for a user menu.
menu single-space	Displays menu items single-spaced rather than double-spaced.
menu status-line	Displays a line of status information about the current user at the top of a menu.
menu text	Specifies the text of a menu item in a user menu.

menu options

To set options for items in user menus, use the **menu options** command in global configuration mode.

menu *menu-name* **options** *menu-item* {**login** | **pause**}

Syntax Description

menu-name	The name of the menu. You can specify a maximum of 20 characters.
menu-item	Number, character, or string key of the item affected by the option.
login	Requires a login before issuing the command.
pause	Pauses after the command is entered before redrawing the menu.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use the **menu command** and **menu text** global configuration commands to define a menu entry.

Examples

In the following example, a login is required before issuing the command specified by menu entry 3 of the menu named Access1:

```
menu Access1 options 3 login
```

Related Commands

Command	Description
menu (EXEC)	Invokes a user menu.
menu clear-screen	Clears the terminal screen before displaying a menu.
menu command	Specifies underlying commands for user menus.
menu default	Specifies the menu item to use as the default.
menu line-mode	Requires the user to press Enter after specifying an item.
menu prompt	Specifies the prompt for a user menu.
menu single-space	Displays menu items single-spaced rather than double-spaced.
menu status-line	Displays a line of status information about the current user at the top of a menu.
menu text	Specifies the text of a menu item in a user menu.
menu title	Creates a title, or banner, for a user menu.

menu prompt

To specify the prompt for a user menu, use the **menu prompt** command in global configuration mode.

menu *menu-name* **prompt** *d prompt d*

Syntax Description

menu-name	Name of the menu. You can specify a maximum of 20 characters.
d	A delimiting character that marks the beginning and end of a title. Text delimiters are characters that do not ordinarily appear within the text of a title, such as slash (/), double quote ("), and tilde (~). ^C is reserved for special use and should not be used in the text of the title.
prompt	Prompt string for the menu.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Press Enter after entering the first delimiter. The router will prompt you for the text of the prompt. Enter the text followed by the delimiter, and press Enter.

Use the **menu command** and **menu text** commands to define the menu selections.

Examples

In the following example, the prompt for the menu named Access1 is configured as “Select an item.”:

```
Router(config)# menu Access1 prompt /
Enter TEXT message.  End with the character '/'.
Select an item. /
Router(config)#
```

Related Commands

Command	Description
menu (EXEC)	Invokes a user menu.
menu command	Specifies underlying commands for user menus.
menu default	Specifies the menu item to use as the default.
menu text	Specifies the text of a menu item in a user menu.
menu title	Creates a title, or banner, for a user menu.

menu single-space

To display menu items single-spaced rather than double-spaced, use the **menu single-space** command in global configuration mode.

menu *menu-name* **single-space**

Syntax Description

menu-name	Name of the menu this command should be applied to.

Defaults

Enabled for menus with more than nine items; disabled for menus with nine or fewer items.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When more than nine menu items are defined, the menu is displayed single-spaced. To configure the menus with nine or fewer items to display single-spaced, use this command.

Examples

In the following example, single-spaced menu items are displayed for the menu named Access1:

```
menu Access1 single-space
```

Related Commands

Command	Description
menu (EXEC)	Invokes a user menu.
menu clear-screen	Clears the terminal screen before displaying a menu.
menu command	Specifies underlying commands for user menus.
menu default	Specifies the menu item to use as the default.
menu line-mode	Requires the user to press Enter after specifying an item.
menu options	Sets options for items in user menus.
menu prompt	Specifies the prompt for a user menu.
menu status-line	Displays a line of status information about the current user at the top of a menu.
menu text	Specifies the text of a menu item in a user menu.
menu title	Creates a title, or banner, for a user menu.

menu status-line

To display a line of status information about the current user at the top of a menu, use the **menu status-line** command in global configuration mode.

menu *menu-name* **status-line**

Syntax Description

menu-name	Name of the menu this command should be applied to.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command displays the status information at the top of the screen before the menu title is displayed. This status line includes the router's host name, the user's line number, and the current terminal type and keymap type (if any).

Examples

In the following example, status information is enabled for the menu named Access1:

```
menu Access1 status-line
```

Related Commands

Command	Description
menu (EXEC)	Invokes a user menu.
menu clear-screen	Clears the terminal screen before displaying a menu.
menu command	Specifies underlying commands for user menus.
menu default	Specifies the menu item to use as the default.
menu line-mode	Requires the user to press Enter after specifying an item in a menu.
menu options	Sets options for items in user menus.
menu prompt	Specifies the prompt for a user menu.
menu single-space	Displays menu items single-spaced rather than double-spaced.
menu text	Specifies the text of a menu item in a user menu.
menu title	Creates a title, or banner, for a user menu.

menu text

To specify the text of a menu item in a user menu, use the **menu text** command in global configuration mode.

menu *menu-name* **text** *menu-item menu-text*

Syntax Description

menu-name	Name of the menu. You can specify a maximum of 20 characters.
menu-item	Number, character, or string used as the key for the item. The key is displayed to the left of the menu item text. You can specify a maximum of 18 menu items. When the tenth item is added to the menu, the **menu line-mode** and **menu single-space** commands are activated automatically.
menu-text	Text of the menu item.

Defaults

No text appears for the menu item.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command to assign text to items in a menu. Use the **menu command** command to assign actions to items. These commands must use the same menu name and menu selection key.

You can specify a maximum of 18 items in a menu.

Examples

In the following example, the descriptive text for the three entries is specified for options 1, 2, and 3 in the menu named Access1:

```
menu Access1 text 1 IBM Information Systems
menu Access1 text 2 UNIX Internet Access
menu Access1 text 3 Exit menu system
```

Related Commands

Command	Description
menu (EXEC)	Invokes a user menu.
menu clear-screen	Clears the terminal screen before displaying a menu.
menu command	Specifies underlying commands for user menus.
menu default	Specifies the menu item to use as the default.
menu line-mode	Requires the user to press Enter after specifying an item.
menu options	Sets options for items in user menus.

Command	Description
menu prompt	Specifies the prompt for a user menu.
menu single-space	Displays menu items single-spaced rather than double-spaced.
menu status-line	Displays a line of status information about the current user at the top of a menu.
menu title	Creates a title, or banner, for a user menu.

menu title

To create a title (banner) for a user menu, use the **menu title** command in global configuration mode.

menu *menu-name* **title** *d menu-title d*

Syntax Description

menu-name	Name of the menu. You can specify a maximum of 20 characters.
d	A delimiting character that marks the beginning and end of a title. Text delimiters are characters that do not ordinarily appear within the text of a title, such as slash (/), double quote ("), and tilde (~). ^C is reserved for special use and should not be used in the text of the title.
menu-title	Lines of text to appear at the top of the menu.

Defaults

The menu does not have a title.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **menu title** command must use the same menu name used with the **menu text** and **menu command** commands used to create a menu.

You can position the title of the menu horizontally by preceding the title text with blank characters. You can also add lines of space above and below the title by pressing Enter.

Follow the **title** keyword with one or more blank characters and a delimiting character of your choice. Then enter one or more lines of text, ending the title with the same delimiting character. You cannot use the delimiting character within the text of the message.

When you are configuring from a terminal and are attempting to include special control characters, such as a screen-clearing string, you must use Ctrl-V before the special control characters so that they are accepted as part of the title string. The string ^[[H^[[J is an escape string used by many VT100-compatible terminals to clear the screen. To use a special string, you must enter Ctrl-V before each escape character.

You also can use the **menu clear-screen** global configuration command to clear the screen before displaying menus and submenus, instead of embedding a terminal-specific string in the menu title. The **menu clear-screen** command allows the same menu to be used on different types of terminals.

Examples

In the following example, the title that will be displayed is specified when the menu named Access1 is invoked. Press Enter after the second slash (/) to display the prompt.

```
Router(config)# menu Access1 title /^[[H^[[J
Enter TEXT message.  End with the character '/'.
               Welcome to Access1 Internet Services
```

```
                    Type a number to select an option;
                            Type 9 to exit the menu.
/
Router(config)#
```

Related Commands

Command	Description
menu (EXEC)	Invokes a user menu.
menu clear-screen	Clears the terminal screen before displaying a menu.
menu command	Specifies underlying commands for user menus.
menu default	Specifies the menu item to use as the default.
menu line-mode	Requires the user to press Enter after specifying an item.
menu options	Sets options for items in user menus.
menu prompt	Specifies the prompt for a user menu.
menu single-space	Displays menu items single-spaced rather than double-spaced.
menu status-line	Displays a line of status information about the current user at the top of a menu.
menu text	Specifies the text of a menu item in a user menu.

microcode (7000/7500)

To specify the location of the microcode that you want to download from Flash memory into the writable control store (WCS) on Cisco 7000 series (including RSP based routers) or Cisco 7500 series routers, use the **microcode** command in global configuration mode. To load the microcode bundled with the system image, use the **no** form of this command.

microcode *interface-type* {*flash-filesystem***:***filename* [*slot*] | **rom** | **system** [*slot*]]}

no microcode *interface-type* {*flash-filesystem***:***filename* [*slot*] | **rom** | **system** [*slot*]}

Syntax Description

interface-type	One of the following interface processor names: **aip**, **cip**, **eip**, **feip**, **fip**, **fsip**, **hip**, **mip**, **sip**, **sp**, **ssp**, **trip**, **vip**, or **vip2**.
*flash-filesystem***:**	Flash file system, followed by a colon. Valid file systems are **bootflash**, **slot0**, and **slot1**. Slave devices such as slaveslot0 are invalid. The slave's file system is not available during microcode reloads.
filename	Name of the microcode file.
slot	(Optional) Number of the slot. Range is from 0 to 15.
rom	If ROM is specified, the router loads from the onboard ROM microcode.
system	If the **system** keyword is specified, the router loads the microcode from the microcode bundled into the system image you are running for that interface type.

Defaults

The default is to load from the microcode bundled in the system image.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

If you do not use the **microcode reload** command after using the **microcode** command, the **microcode reload** command will be written to the configuration file automatically.

When using Dual RSPs for simple hardware backup, ensure that the master and slave RSP card contain the same microcode image in the same location when the router is to load the interface processor microcode from a Flash file system. Thus, if the slave RSP becomes the master, it will be able to find the microcode image and download it to the interface processor.

Examples

In the following example, all FIP cards will be loaded with the microcode found in Flash memory file fip.v141-7 when the system is booted, when a card is inserted or removed, or when the **microcode reload** global configuration command is issued. The configuration is then written to the startup configuration file.

```
Router(config)# microcode fip slot0:fip.v141-7
Router(config)# end
Router# copy system:running-config nvram:startup-config
```

Related Commands

Command	Description
more flh:logfile	Displays the system console output generated during the Flash load helper operation.

microcode (12000)

To load a Cisco IOS software image on a line card from Flash memory or the GRP card on a Cisco 12000 series Gigabit Switch Router (GSR), use the **microcode** command in global configuration mode. To load the microcode bundled with the GRP system image, use the **no** form of this command.

microcode {**oc12-atm** | **oc12-pos | oc3-pos4**} {**flash** *file-id* [*slot*] | **system** [*slot*]}

no microcode {**oc12-atm** | **oc12-pos** | **oc3-pos4**} [**flash** *file-id* [*slot*] | **system** [*slot*]]

Syntax Description

oc12-atm | oc12-pos | oc3-pos4	Interface name.
flash	Loads the image from the Flash file system.
file-id	Specifies the device and filename of the image file to download from Flash memory. A colon (:) must separate the device and filename (for example, slot0:gsr-p-mz). Valid devices include: • **bootflash:**—Internal Flash memory. • **slot0:**—First PCMCIA slot. • **slot1:**—Second PCMCIA slot.
slot	(Optional) Slot number of the line card that you want to copy the software image to. Slot numbers range from 0 to 11 for the Cisco 12012 router and 0 to 7 for the Cisco 12008 router. If you do not specify a slot number, the Cisco IOS software image is downloaded on all line cards.
system	Loads the image from the software image on the GRP card.

Defaults

The default is to load the image from the GRP card (**system**).

Command Modes

Global configuration

Command History

Release	Modification
11.2 GS	This command was introduced for Cisco 12000 series GSRs.

Usage Guidelines

In addition to the Cisco IOS image that resides on the GRP card, each line card on a Cisco 12000 series has a Cisco IOS image. When the router is reloaded, the specified image is loaded onto the GRP card and then automatically downloaded to all the line cards.

Normally, you want the same Cisco IOS image on the GRP card and all line cards. However, if you want to upgrade a line card with a new version of microcode for testing or to fix a defect, you might need to load a Cisco IOS image that is different from the one on the line card. Additionally, you might need to load a new image on the line card to work around a problem that is affecting only one of the line cards.

To load a Cisco IOS image on a line card, first use the **copy tftp** command to download the Cisco IOS image to a slot on one of the PCMCIA Flash memory cards. Then use the **microcode** command to download the image to the line card, followed by the **microcode reload** command to start the image. Immediately after you enter the **microcode reload** command and press Return, the system reloads all microcode. Global configuration mode remains enabled. After the reloading is complete, enter the **exit** command to return to the EXEC system prompt.

To verify that the correct image is running on the line card, use the **execute-on slot** *slot* **show version** command.

For additional information on GSR configuration, refer to the documentation specific to your Cisco IOS software release.

Examples

In the following example, the Cisco IOS software image in slot 0 is downloaded to the line card in slot 10. This software image is used when the system is booted, a line card is inserted or removed, or the **microcode reload** global configuration command is issued.

```
Router(config)# microcode oc3-POS-4 flash slot0:fip.v141-7 10
Router(config)# microcode reload 10
```

In this example, the user would issue the **execute-on slot 10 show version** command to verify that the correct version is loaded.

Related Commands

Command	Description
microcode reload (12000)	Reloads microcode on Cisco 12000 series GSRs.

microcode (7200)

To configure a default override for the microcode that is downloaded to the hardware on a Cisco 7200 series router, use the **microcode** command in global configuration mode. To revert to the default microcode for the current running version of the Cisco IOS software, use the **no** form of this command.

microcode {**ecpa** | **pcpa**} *location*

no microcode {**ecpa** | **pcpa**}

Syntax Description

ecpa	ESCON Channel Port Adapter (CPA) interface.
pcpa	Parallel CPA interface.
location	Location of microcode, including the device and filename.

Defaults

If the default or **no** form of the command is specified, the driver uses the default microcode for the current running version of the Cisco IOS software.

Command Modes

Global configuration

Command History

Release	Modification
11.3(3)T	This command was introduced.

Usage Guidelines

If there are any default overrides when the configuration is written, then the **microcode reload** command will be written to the configuration automatically. This action enables the configured microcode to be downloaded at system startup.

The CPA microcode image is preloaded on Flash memory cards for Cisco 7200-series routers for Cisco IOS Release 11.3(3)T and later releases. You may be required to copy a new image to Flash memory when a new microcode image becomes available.

For more information on the CPA configuration and maintenance, refer to the "Configuring Cisco Mainframe Channel Connection Adapters" chapter in the *Cisco IOS Bridging and IBM Networking Configuration Guide*.

Examples

The following example instructs the Cisco IOS software to load the microcode from an individual microcode image that is stored as a file on the Flash card inserted in Flash card slot 0:

```
microcode ecpa slot0:xcpa26-1
```

Related Commands

Command	Description
microcode reload (7200)	Resets and reloads the specified hardware in a Cisco 7200 series router.
show microcode	Displays microcode information.

microcode reload (7000/7500)

To reload the processor card on the Cisco 7000 series with RSP7000 or Cisco 7500 series routers, use the **microcode reload** command in global configuration mode.

microcode reload

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced for Cisco 7500 series routers.

Usage Guidelines

This command reloads the microcode without rebooting the router. Immediately after you enter the **microcode reload** command and press Return, the system reloads all microcode. Global configuration mode remains enabled.

Note If you modify the system configuration to load a microcode image, the **microcode reload** command will be written to the configuration file automatically following the use of a **microcode** command. This action enables the configured microcode to be downloaded at system startup.

Examples

In the following example, all controllers are reset, and the microcode specified in the current configuration is loaded:

```
Router(config)# microcode reload
```

Related Commands

Command	Description
microcode (7000/7500)	Specifes the location from where microcode should be loaded when the **microcode reload** command is executed on RSP-based routers.

microcode reload (7200)

To reload the Cisco IOS microcode image on an ESCON CPA card in the Cisco 7200 series router, use the **microcode reload** command in privileged EXEC mode.

microcode reload {**all** | **ecpa** [**slot** *slot-number*] | **pcpa** [**slot** *slot-number*]}

Syntax Description

all	Resets and reloads all hardware types that support downloadable microcode.
ecpa	Resets and reloads only those slots that contain hardware type **ecpa**.
pcpa	Resets and reloads only those slots that contain hardware type **pcpa**.
slot *slot-number*	(Optional) Resets and reloads only the slot specified, and only if it contains the hardware specified.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(3)T	This command was introduced.

Usage Guidelines

Hardware types that do not support downloadable microcode are unaffected by the **microcode reload all** command.

You will be prompted for confirmation before the **microcode reload** command is executed.

Examples

The following example reloads the ESCON CPA microcode in slot 5 with the currently configured microcode:

```
Router# microcode reload ecpa slot 5
```

Related Commands

Command	Description
microcode (7200)	Configures a default override for the microcode that is downloaded to the hardware on a Cisco 7200 series router.
show microcode	Displays the microcode bundled into a Cisco 7000 series with RSP7000, Cisco 7200 series, or Cisco 7500 series router.

microcode reload (12000)

To reload the Cisco IOS image from a line card on Cisco 12000 series routers, use the **microcode reload** command in global configuration mode.

microcode reload [*slot-number*]

Syntax Description

slot-number	(Optional) Slot number of the line card that you want to reload the Cisco IOS software image on. Slot numbers range from 0 to 11 for the Cisco 12012 and from 0 to 7 for the Cisco 12008 router. If you do not specify a slot number, the Cisco IOS software image is reloaded on all line cards.

Command Modes

Global configuration

Command History

Release	Modification
11.2 GS	This command was introduced for Cisco 12000 series GSRs.

Usage Guidelines

In addition to the Cisco IOS image that resides on the GRP card, each line card on Cisco 12000 series routers has a Cisco IOS image. When the router is reloaded, the specified Cisco IOS image is loaded onto the GRP card and automatically downloaded to all the line cards.

Normally, you want the same Cisco IOS image on the GRP card and all line cards. However, if you want to upgrade a line card with a new version of microcode for testing or to fix a defect, you might need to load a different Cisco IOS image. Additionally, you might need to load a new image on the line card to work around a problem affecting only one of the line cards.

To load a Cisco IOS image on a line card, first use the **copy tftp** command to download the Cisco IOS image to a slot on one of the PCMCIA Flash memory cards. Then use the **microcode** command to download the image to the line card, followed by the **microcode reload** command to start the image. To verify that the correct image is running on the line card, use the **execute-on slot** *slot* **show version** command.

For additional information on GSR configuration, refer to the "Observing System Startup and Performing a Basic Configuration" chapter in the Cisco 12000 series installation and configuration guides.

The **microcode reload** (12000) command allows you to issue another command immediately.

Note Issuing a **microcode reload** command on any of the line cards in a Cisco 12000 GSR immediately returns the console command prompt. This allows you to issue a subsequent command immediately to the reloading line card. However, any commands entered at this time will not execute, and often no indication will be given that such a command failed to run. Verify that the microcode has reloaded before issuing new commands.

Examples

In the following example, the mirocode firmware is reloaded on the line card in slot 10:

```
Router(config)# microcode reload 10
```

Related Commands

Command	Description
microcode (12000)	Loads a Cisco IOS software image on a line card from Flash memory or the GRP card on a Cisco 12000 series GSR.

mkdir

To create a new directory in a Class C Flash file system, use the **mkdir** command in EXEC mode.

mkdir *directory*

Syntax Description

directory	The name of the directory to create.

Command Modes

EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.

Usage Guidelines

This command is only valid on Class C Flash file systems.

If you do not specify the directory name in the command line, the router prompts you for it.

Examples

The following example creates a directory named newdir:

```
Router# mkdir newdir

Mkdir file name [newdir]?
Created dir flash:newdir
Router# dir
Directory of flash:

  2  drwx           0   Mar 13 1993 13:16:21  newdir

8128000 bytes total (8126976 bytes free)
```

Related Commands

Command	Description
dir	Displays a list of files on a file system.
rmdir	Removes an existing directory in a Class C Flash file system.

mop device-code

To identify the type of device sending Maintenance Operation Protocol (MOP) System Identification (sysid) messages and request program messages, use the **mop device-code** command in global configuration mode. To set the identity to the default value, use the **no** form of this command.

mop device-code {**cisco** | **ds200**}

no mop device-code {**cisco** | **ds200**}

Syntax Description

cisco	Denotes a Cisco device code. This is the default.
ds200	Denotes a DECserver 200 device code.

Defaults

Cisco device code

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The sysid messages and request program messages use the identity information indicated by this command.

Examples

The following example identifies a DECserver 200 device as sending MOP sysid and request program messages:

```
mop device-code ds200
```

Related Commands

Command	Description
mop sysid	Enables an interface to send out periodic MOP system identification messages.

mop retransmit-timer

To configure the length of time that the Cisco IOS software waits before resending boot requests to a Maintenance Operation Protocol (MOP) server, use the **mop retransmit-timer** command in global configuration mode. To reinstate the default value, use the **no** form of this command.

mop retransmit-timer *seconds*

no mop retransmit-timer

Syntax Description

seconds	Sets the length of time (in seconds) that the software waits before resending a message. The value is a number from 1 to 20.

Defaults

4 seconds

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

By default, when the software sends a request that requires a response from a MOP boot server and the server does not respond, the message is re-sent after 4 seconds. If the MOP boot server and router are separated by a slow serial link, it might take longer than 4 seconds for the software to receive a response to its message. Therefore, you might want to configure the software to wait longer than 4 seconds before resending the message if you are using such a link.

Examples

In the following example, if the MOP boot server does not respond within 10 seconds after the router sends a message, the server will resend the message:

```
mop retransmit-timer 10
```

Related Commands

Command	Description
mop device-code	Identifies the type of device sending MOP sysid messages and requests program messages.
mop enabled	Enables an interface to support the MOP.

mop retries

To configure the number of times the Cisco IOS software will resend boot requests to a Maintenance Operation Protocol (MOP) server, use the **mop retries** command in global configuration mode. To reinstate the default value, use the **no** form of this command.

mop retries *count*

no mop retries

Syntax Description

count	Indicates the number of times the software will resend a MOP boot request. The value is a number from 3 to 24. The default is 8.

Defaults

8 times

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

In the following example, the software will attempt to resend a message to an unresponsive host 11 times before declaring a failure:

```
Router(config)# mop retries 11
```

Related Commands

Command	Description
mop device-code	Identifies the type of device sending MOP sysid messages and requests program messages.
mop enabled	Enables an interface to support the MOP server.
mop retransmit-timer	Configures the length of time that the Cisco IOS software waits before resending boot requests to a MOP server.

more

To display a file, use the **more** command in EXEC mode.

more [**/ascii** | **/binary** | **/ebcdic**] *file-url*

Syntax Description

/ascii	(Optional) Displays a binary file in ASCII format.
/binary	(Optional) Displays a file in hex/text format.
/ebcdic	(Optional) Displays a binary file in EBCDIC format.
file-url	The URL of the file to display.

Command Modes

EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.

Usage Guidelines

The **more system:running-config** command displays the same output as the **show running-config** command. The **more nvram:startup-config** command replaces the **show startup-config** command and the **show configuration** command.

You can use this command to display configuration files, as follows:

- The **more nvram:startup-config** command displays the startup configuration file contained in NVRAM or specified by the CONFIG_FILE environment variable. The Cisco IOS software informs you whether the displayed configuration is a complete configuration or a distilled version. A distilled configuration is one that does not contain access lists.
- The **more system:running-config** command displays the running configuration.

These commands show the version number of the software used when you last changed the configuration file.

You can display files on remote systems using the **more** command.

Examples

The following partial sample output displays the configuration file named startup-config in NVRAM:

```
Router# more nvram:startup-config

!
! No configuration change since last restart
! NVRAM config last updated at 02:03:26 PDT Thu Oct 2 1997
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
service password-encryption
service udp-small-servers
service tcp-small-servers
```

```
.
.
.
end
```

The following is partial sample output from the **more nvram:startup-config** command when the configuration file has been compressed:

```
Router# more nvram:startup-config

Using 21542 out of 65536 bytes, uncompressed size = 142085 bytes
!
version 12.1
service compress-config
!
hostname rose
!
.
.
.
```

The following partial sample output displays the running configuration:

```
Router2# more system:running-config

Building configuration...

Current configuration:
!
version 12.1
no service udp-small-servers
no service tcp-small-servers
!
hostname Router2
!
.
.
.
!
end
```

Related Commands

Command	Description
boot config	Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).
service compress-config	Compresses startup configuration files.
show bootvar	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.

more <url> begin

To search the output of any **more** command, use the **more** *url* **|** **begin** command in EXEC mode. This command begins unfiltered output of the **more** command with the first line that contains the regular expression you specify.

more *url* **|** **begin** *regular-expression*

Syntax Description

url	The Universal Resource Locator (RLl) of the file to display. **More** commands are advanced **show** commands; for details, see the command reference page in this book for the **more** command.
|	A vertical bar (the "pipe" symbol) indicates that an output processing specification follows.
regular-expression	Any regular expression found in **more** command output.
/	Specifies a search at a --More-- prompt that begins unfiltered output with the first line that contains the regular expression.
-	Specifies a filter at a --More-- prompt that only displays output lines that do not contain the regular expression.
+	Specifies a filter at a --More-- prompt that only displays output lines that contain the regular expression.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
11.3 AA	The **more** command was introduced.
12.0(1)T	This extension of the **more** command was introduced.

Usage Guidelines

The *regular-expression* argument is case sensitive and allows for complex matching requirements.

You can specify a new search at every --More-- prompt.

To search the remaining output of the **more** command, use the following command at the --More-- prompt:

/regular-expression

To filter the remaining output of the **more** command, use one of the following commands at the --More-- prompt:

-regular-expression

+regular-expression

When output volume is large, the search can produce long lists of output. To interrupt the output, press **Ctrl**-^ (Ctrl-Shift-6) or **Ctrl**-**Z**.

Note Once you specify a filter for a **more** command, you cannot specify another filter at a --More-- prompt. The first specified filter remains until the **more** command output finishes or until you interrupt the output. The use of the keyword **begin** does not constitute a filter.

Because prior output is not saved, you cannot search or filter backward through prior output.

Examples

The following is partial sample output of the **more nvram:startup-config | begin** command that begins unfiltered output with the first line that contain the regular expression "ip." At the --More-- prompt, the user specifies a filter to exclude output lines that contain the regular expression "ip."

```
router# more nvram:startup-config | begin ip

ip subnet-zero
ip domain-name cisco.com
ip name-server 198.92.30.32
ip name-server 171.69.2.132
!
isdn switch-type primary-5ess
.
.
.
interface Ethernet1
 ip address 5.5.5.99 255.255.255.0
 --More--
-ip
filtering...
 media-type 10BaseT
!
interface Serial0:23
 encapsulation frame-relay
 no keepalive
 dialer string 4001
 dialer-group 1
 isdn switch-type primary-5ess
 no fair-queue
```

Related Commands

Command	Description
more <url> exclude	Filters **more** command output so that it excludes lines that contain a particular regular expression.
more <url> include	Filters **more** command output so that it displays only lines that contain a particular regular expression.
show <command> begin	Searches the output of any **show** command and displays the output from the first instance of a specified string.
show <command> exclude	Filters **show** command output so that it excludes lines that contain a particular regular expression.
show <command> include	Filters **show** command output so that it displays only lines that contain a particular regular expression.

more <url> exclude

To filter **more** command output so that it excludes lines that contain a particular regular expression, use the **more exclude** command in EXEC mode.

more *url* **| exclude** *regular-expression*

Syntax Description

url	The Universal Resource Locator (URL) of the file to display. **More** commands are advanced **show** commands; for details, see the command reference page in this book for the **more** command. The Cisco IOS File System (IFS) uses URLs to specify the location of a file system, directory, and file. Typical URL elements include: *prefix***:**[*directory*/]*filename* Prefixes can be local file systems or file locations, such as **nvram:** or **system:**. Alternatively, you can specify network locations using the following syntax: **ftp:**[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename* **tftp:**[[//*location*]/*directory*]/*filename* **rcp:**[[//[*username@*]*location*]/*directory*]/*filename*
|	A vertical bar (the "pipe" symbol) indicates that an output processing specification follows.
regular-expression	Any regular expression found in **more** command output.
/	Specifies a search at a --More-- prompt that begins unfiltered output with the first line that contains the regular expression.

Command Modes

EXEC

Command History

Release	Modification
11.3 AA	The **more** command was introduced.
12.0(1)T	This extension of the **more** command was introduced.

Usage Guidelines

The *regular-expression* argument is case sensitive and allows for complex matching requirements.

You can specify a new search at any --More-- prompt. To search the remaining output of the **more** command, use the following command at the --More-- prompt:

/regular-expression

When output volume is large, the search can produce long lists of output. To interrupt the output, press **Ctrl**-^ (Ctrl-Shift-6) or **Ctrl**-**Z**.

Because prior output is not saved, you cannot search or filter backward through prior output.

Examples

The following is partial sample output of the **more nvram:startup-config | exclude** command. The use of **| exclude service** in the command specifies a filter that excludes lines that contain the regular expression "service." At the --More-- prompt, the user searches for the regular expression "Dialer1," which continues filtered output with the first line that contains "Dialer1."

```
router# more nvram:startup-config | exclude service
!
version 12.0
!
hostname router
!
boot system flash
no logging buffered
!
ip subnet-zero
ip domain-name cisco.com
.
.
.
--More--
/Dialer1
filtering...
interface Dialer1
 no ip address
 no ip directed-broadcast
 dialer in-band
 no cdp enable
```

Related Commands

Command	Description
more <url> begin	Begins unfiltered output of the **more** command with the first line that contains the regular expression you specify.
more <url> include	Filters **more** command output so that it displays only lines that contain a particular regular expression.
show <command> begin	Searches the output of any **show** command and displays the output from the first instance of a specified string.
show <command> exclude	Filters **show** command output so that it excludes lines that contain a particular regular expression.
show <command> include	Filters **show** command output so that it displays only lines that contain a particular regular expression.

more <url> include

To filter **more** command output so that it displays only lines that contain a particular regular expression, use the **more include** command in EXEC mode.

more *url* **| include** *regular-expression*

Syntax Description

url	The Universal Resource Locator (URL) of the file to display. **More** commands are advanced **show** commands; for details, see the command reference page in this book for the **more** command.
|	A vertical bar (the "pipe" symbol) indicates that an output processing specification follows.
regular-expression	Any regular expression found in **more** command output.
/	Specifies a search at a --More-- prompt that begins unfiltered output with the first line that contains the regular expression.

Command Modes

EXEC

Command History

Release	Modification
11.3 AA	The **more** command was introduced.
12.0(1)T	This extension of the **more** command was introduced.

Usage Guidelines

The *regular-expression* argument is case sensitive and allows for complex matching requirements.

You can specify a new search at any --More-- prompt. To search the remaining output of the **more** command, use the following syntax at the --More-- prompt:

/regular-expression

When output volume is large, the search can produce long lists of output. To interrupt the output, press **Ctrl**-^ (Ctrl-Shift-6) or **Ctrl**-**Z**.

Because prior output is not saved, you cannot search or filter backward through prior output.

Examples

The following is partial sample output of the **more nvram:startup-config | include** command. It only displays lines that contain the regular expression "ip."

```
router# more nvram:startup-config | include ip

ip subnet-zero
ip domain-name cisco.com
ip name-server 198.92.30.32
ip name-server 171.69.2.132
 description ip address 172.21.53.199 255.255.255.0
 ip address 172.21.53.199 255.255.255.0
```

Related Commands

Command	Description
more <url> begin	Begins unfiltered output of the **more** command with the first line that contains the regular expression you specify.
more <url> exclude	Filters **more** command output so that it excludes lines that contain a particular regular expression.
show <command> begin	Searches the output of any **show** command and displays the output from the first instance of a specified string.
show <command> exclude	Filters **show** command output so that it excludes lines that contain a particular regular expression.
show <command> include	Filters **show** command output so that it displays only lines that contain a particular regular expression.

motd-banner

To enable the display of message-of-the-day (MOTD) banners on the specified line or lines, use the **motd-banner** command in line configuration mode. To suppress the MOTD banners on the specified line or lines, use the **no** form of this command.

motd-banner

no motd-banner

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled on all lines.

Command Modes

Line configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command determines whether the router will display the MOTD banner when an EXEC session is created on the specified line or lines. The MOTD banner is defined with the **banner motd** global configuration command. By default, the MOTD banner is enabled on all lines. Disable the MOTD banner on specific lines using the **no motd-banner** line configuration command.

The MOTD banners can also be disabled by the **no exec-banner** line configuration command, which disables both MOTD banners and EXEC banners on a line. If the **no exec-banner** command is configured on a line, the MOTD banner will be disabled regardless of whether the **motd-banner** command is enabled or disabled. Table 34 summarizes the effects of the **exec-banner** command and the **motd-banner** command.

Table 34 Banners Displayed Based On exec-banner and motd-banner Combinations

	exec-banner (default)	**no exec-banner**
motd-banner (default)	MOTD banner EXEC banner	None
no motd-banner	EXEC banner	None

For reverse Telnet connections, the EXEC banner is never displayed. Instead, the incoming banner is displayed. The MOTD banner is displayed by default, but it is disabled if either the **no exec-banner** command or **no motd-banner** command is configured. Table 35 summarizes the effects of the **exec-banner** command and the **motd-banner** command for reverse Telnet connections.

Table 35 Banners Displayed Based On exec-banner and motd-banner Combinations for Reverse Telnet Sessions to Async Lines

	exec-banner (default)	**no exec-banner**
motd-banner (default)	MOTD banner Incoming banner	Incoming banner
no motd-banner	Incoming banner	Incoming banner

Examples

The following example suppresses the MOTD banner on vty lines 0 through 4:

```
line vty 0 4
 no motd-banner
```

Related Commands

Command	Description
banner exec	Defines and enables a customized banner to be displayed whenever the EXEC process is initiated.
banner incoming	Defines and enables a customized message to be displayed when there is an incoming connection to a terminal line from a host on the network.
banner motd	Defines and enables a customized message-of-the-day banner.
motd-banner	Controls (enables or disables) the display of message-of-the-day banners on a specified line or lines.

name-connection

To assign a logical name to a connection, use the **name-connection** command in user EXEC mode.

name-connection

Syntax Description

This command has no arguments or keywords.

Defaults

No logical name is defined.

Command Modes

User EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command can be useful for keeping track of multiple connections.

You are prompted for the connection number and name to assign. The **where** command displays a list of the assigned logical connection names.

Examples

The following example assigns the logical name blue to the connection:

```
Router> where
Conn Host                Address             Byte  Idle Conn Name
*  1 doc-2509            172.30.162.131         0     0 doc-2509

Router> name-connection
Connection number: 1
Enter logical name: blue
Connection 1 to doc-2509 will be named "BLUE" [confirm]
```

Related Commands

Command	Description
where	Lists open sessions associated with the current terminal line.

no menu

To delete a user menu from the configuration file, use the **no menu** command in global configuration mode.

no menu *menu-name*

Syntax Description

menu-name	Name of the menu to delete from the configuration file.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command to remove any **menu** commands for a particular menu from the configuration file.

As with all global configuration commands, this command will only effect the startup configuration file when you save the running configuration using the **copy running-config startup-config** EXEC command.

Examples

The following example deletes the menu named Access1:

```
no menu Access1
```

Related Commands

Command	Description
menu (EXEC)	Invokes a user menu.
menu command	Specifies underlying commands for user menus.
menu prompt	Specifies the prompt for a user menu.
menu text	Specifies the text of a menu item in a user menu.
menu title	Creates a title, or banner, for a user menu.

no snmp-server

To disable Simple Network Management Protocol (SNMP) agent operation, use the **no snmp-server** command in global configuration mode.

no snmp-server

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command disables all running versions of SNMP (SNMPv1, SNMPv2C, and SNMPv3) on the device.

Examples

The following example disables the current running version of SNMP:

```
Router(config)# no snmp-server
```

notify

To enable terminal notification about pending output from other Telnet connections, use the **notify** command in line configuration mode. To disable notifications, use the **no** form of this command.

notify

no notify

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command sets a line to inform a user that has multiple, concurrent Telnet connections when output is pending on a connection other than the current one.

Examples

In the following example, notification of pending output from connections is enabled on virtual terminal lines 0 to 4:

```
Router(config)# line vty 0 4
Router(config-line)# notify
```

Related Commands

Command	Description
terminal notify	Configures a line to inform a user that has multiple, concurrent Telnet connections when output is pending on a connection other than the current one.

ntp access-group

To control access to the Network Time Protocol (NTP) services on the system, use the **ntp access-group** command in global configuration mode. To remove access control to the NTP services, use the **no** form of this command.

ntp access-group {**query-only** | **serve-only** | **serve** | **peer**} *access-list-number*

no ntp access-group {**query-only** | **serve-only** | **serve** | **peer**}

Syntax Description

query-only	Allows only NTP control queries. See RFC 1305 (NTP version 3).
serve-only	Allows only time requests.
serve	Allows time requests and NTP control queries, but does not allow the system to synchronize to the remote system.
peer	Allows time requests and NTP control queries and allows the system to synchronize to the remote system.
access-list-number	Number (from 1 to 99) of a standard IP access list.

Defaults

No access control (full access granted to all systems)

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The access group options are scanned in the following order from least restrictive to most restrictive:

1. **peer**
2. **serve**
3. **serve-only**
4. **query-only**

Access is granted for the first match that is found. If no access groups are specified, all access is granted to all sources. If any access groups are specified, only the specified access is granted. This facility provides minimal security for the time services of the system. However, it can be circumvented by a determined programmer. If tighter security is desired, use the NTP authentication facility.

Examples

The following example configures the system to allow itself to be synchronized by a peer from access list 99. However, the system restricts access to allow only time requests from access list 42.

```
Router(config)# ntp access-group peer 99
Router(config)# ntp access-group serve-only 42
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.

ntp authenticate

To enable Network Time Protocol (NTP) authentication, use the **ntp authenticate** command in global configuration mode. To disable the function, use the **no** form of this command.

ntp authenticate

no ntp authenticate

Syntax Description

This command has no arguments or keywords.

Defaults

No authentication

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command if you want authentication. If this command is specified, the system will not synchronize to a system unless it carries one of the authentication keys specified in the **ntp trusted-key** global configuration command.

Examples

The following example configures the system to synchronize only to systems that provide authentication key 42 in their NTP packets:

```
Router(config)# ntp authenticate
Router(config)# ntp authentication-key 42 md5 aNiceKey
Router(config)# ntp trusted-key 42
```

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp trusted-key	Authenticates the identity of a system to which NTP will synchronize.

ntp authentication-key

To define an authentication key for Network Time Protocol (NTP), use the **ntp authentication-key** command in global configuration mode. To remove the authentication key for NTP, use the **no** form of this command.

ntp authentication-key *number* **md5** *value*

no ntp authentication-key *number*

Syntax Description

number	Key number (from 1 to 4294967295).
md5	Authentication key. Message authentication support is provided using the message digest algorithm 5 (MD5) algorithm. The key type **md5** is currently the only key type supported.
value	Key value (an arbitrary string of up to eight characters).

Defaults

No authentication key is defined for NTP.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command to define authentication keys for use with other NTP commands in order to provide a higher degree of security.

Note When this command is written to NVRAM, the key is encrypted so that it is not displayed when the configuration is viewed.

Examples

The following example configures the system to synchronize only to systems providing authentication key 42 in their NTP packets:

```
Router(config)# ntp authenticate
Router(config)# ntp authentication-key 42 md5 aNiceKey
Router(config)# ntp trusted-key 42
```

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp peer	Configures the software clock to synchronize a peer or to be synchronized by a peer.
ntp server	Allows the software clock to be synchronized by a time server.
ntp trusted-key	Authenticates the identity of a system to which NTP will synchronize.

ntp broadcast

To configure the system to send Network Time Protocol (NTP) broadcast packets on a specified interface, use the **ntp broadcast** command in interface configuration mode. To disable this capability, use the **no** form of this command.

ntp broadcast [**version** *number*]

no ntp broadcast

Syntax Description

version *number*	(Optional) Number from 1 to 3 indicating the NTP version.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example configures Ethernet interface 0 to send NTP version 2 broadcasts:

```
Router(config)# interface ethernet 0
Router(config-if)# ntp broadcast version 2
```

Related Commands

Command	Description
ntp broadcast client	Allows the system to receive NTP broadcast packets on an interface.
ntp broadcastdelay	Sets the estimated round-trip delay between the Cisco IOS software and an NTP broadcast server.

ntp broadcast client

To configure the system to receive Network Time Protocol (NTP) broadcast packets on a specified interface, use the **ntp broadcast client** command in interface configuration mode. To disable this capability, use the **no** form of this command.

ntp broadcast client

no ntp broadcast client

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command to allow the system to listen to broadcast packets on an interface-by-interface basis.

Examples

In the following example, the system is configured to receive (listen to) NTP broadcasts on Ethernet interface 1:

```
Router(config)# interface ethernet 1
Router(config-if)# ntp broadcast client
```

Related Commands

Command	Description
ntp broadcast	Configures the specified interface to send NTP broadcast packets.
ntp broadcastdelay	Sets the estimated round-trip delay between the system and an NTP broadcast server.

ntp broadcastdelay

To set the estimated round-trip delay between the Cisco IOS software and a Network Time Protocol (NTP) broadcast server, use the **ntp broadcastdelay** command in global configuration mode. To revert to the default value, use the **no** form of this command.

ntp broadcastdelay *microseconds*

no ntp broadcastdelay

Syntax Description

microseconds	Estimated round-trip time (in microseconds) for NTP broadcasts. The range is from 1 to 999999.

Defaults

3000 microseconds

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command when the router is configured as a broadcast client and the round-trip delay on the network is other than 3000 microseconds.

Examples

The following example sets the estimated round-trip delay between a router and the broadcast client to 5000 microseconds:

```
Router(config)# ntp broadcastdelay 5000
```

Related Commands

Command	Description
ntp broadcast	Configures the specified interface to send NTP broadcast packets.
ntp broadcast client	Configures the specified interface to receive NTP broadcast packets.

ntp clock-period

Caution Do not enter this command; it is documented for informational purposes only. The system automatically generates this command as Network Time Protocol (NTP) determines the clock error and compensates.

As NTP compensates for the error in the software clock, it keeps track of the correction factor for this error. The system automatically saves this value into the system configuration using the **ntp clock-period** command in global configuration mode. To revert to the default, use the **no** form of this command.

ntp clock-period *value*

no ntp clock-period

Syntax Description

value	Amount to add to the software clock for each clock hardware tick (this value is multiplied by 2^{-32}).

Defaults

17179869 2^{-32} seconds (4 milliseconds)

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Do not manually set a value for the NTP clock-period.

If a **copy running-config startup-config** command is entered to save the configuration to NVRAM, the **ntp clock-period** command will automatically be added to the startup configuration. We recommend saving the running configuration to the startup configuration after NTP has been running for a week or so specifically for the purpose of capturing the current setting for the clock-period; performing this task will help NTP synchronize more quickly if the system is restarted.

Examples

The following example shows a typical difference between the values of the NTP clock-period setting in the running configuration and the startup configuration:

```
Router# show startup-config | include clock-period

ntp clock-period 17180239

Router# show running-config | include clock-period

ntp clock-period 17180255
```

ntp disable

To prevent an interface from receiving Network Time Protocol (NTP) packets, use the **ntp disable** command in interface configuration mode. To enable receipt of NTP packets on an interface, use the **no** form of this command.

ntp disable

no ntp disable

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command provides a simple method of access control.

Examples

The following example prevents Ethernet interface 0 from receiving NTP packets:

```
Router(config)# interface ethernet 0
Router(config-if)# ntp disable
```

ntp master

To configure the Cisco IOS software as a Network Time Protocol (NTP) master clock to which peers synchronize themselves when an external NTP source is not available, use the **ntp master** command in global configuration mode. To disable the master clock function, use the **no** form of this command.

ntp master [*stratum*]

no ntp master [*stratum*]

Caution Use this command with caution. It is very easy to override valid time sources using this command, especially if a low stratum number is configured. Configuring multiple machines in the same network with the **ntp master** command can cause instability in keeping time if the machines do not agree on the time.

Syntax Description

stratum	(Optional) Number from 1 to 15. Indicates the NTP stratum number that the system will claim.

Defaults

By default, the master clock function is disabled. When enabled, the default stratum is 8.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Because the Cisco implementation of NTP does not support directly attached radio or atomic clocks, the router is normally synchronized, directly or indirectly, to an external system that has such a clock. In a network without Internet connectivity, such a time source may not be available. The **ntp master** command is used in such cases.

If the system has **ntp master** configured, and it cannot reach any clock with a lower stratum number, the system will claim to be synchronized at the configured stratum number, and other systems will be willing to synchronize to it via NTP.

Note The software clock must have been set from some source, including manually, before the **ntp master** command will have any effect. This protects against distributing erroneous time after the system is restarted.

Examples

The following example configures a router as an NTP master clock to which peers may synchronize:

```
Router(config)# ntp master 10
```

Related Commands

Command	Description
clock calendar-valid	Configures the system hardware clock an authoritative time source for the network.

ntp max-associations

To configure the maximum number of Network Time Protocol (NTP) peers and clients for the routing device, use the **ntp max-associations** command in global configuration mode. To return the maximum associations value to the default, use the **no** form of this command.

ntp max-associations *number*

no ntp max-associations

Syntax Description

number	Specifies the number of NTP associations. The range is 0 to 4294967295. The default is 100.

Defaults

100 maximum associations.

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The router can be configured to define the maximum number of NTP peer and client associations that the router will serve. The **ntp max-associations** command is used to set this limit.

This command is useful for ensuring that that the router is not overwhelmed by huge numbers of NTP synchronization requests or, for an NTP master server, to allow large numbers of devices to sync to the router.

Examples

In the following example, the router is configured so that it can act as an NTP server to 200 clients:

```
Router(config)# ntp max-associations 200
```

Related Commands

Command	Description
show ntp associations	Shows all current NTP associations for the device.

ntp multicast

To configure the system to send Network Time Protocol (NTP) multicast packets on a specified interface, use the **ntp multicast** interface configuration command. To disable this capability, use the **no** form of this command.

ntp multicast [*ip-address*] [**key** *key-id*] [**ttl** *value*] [**version** *number*]

no ntp multicast [*ip-address*]

Syntax Description

ip-address	(Optional) IP address of the multicast group. Default address is 224.0.1.1.
key	(Optional) Defines a multicast authentication key.
key-id	(Optional) Authentication key number in the range from 1 to 4294967295.
ttl	(Optional) Defines the time-to-live (TTL) value of a multicast NTP packet.
value	(Optional) TTL value in the range from 1 to 255. Default TTL value is 16.
version	(Optional) Defines the NTP version number.
number	(Optional) NTP version number in the range from 1 to 3. Default version number is 3.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

The TTL value is used to limit the scope of an audience for multicast routing.

Examples

The following example configures Ethernet interface 0 to send NTP version 2 broadcasts:

```
Router(config)# interface ethernet 0
Router(config-if)# ntp multicast version 2
```

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp multicast client	Allows the system to receive NTP multicast packets on an interface.

ntp multicast client

To configure the system to receive Network Time Protocol (NTP) multicast packets on a specified interface, use the **ntp multicast client** interface configuration command. To disable this capability, use the **no** form of this command.

ntp multicast client [*ip-address*]

no ntp multicast client [*ip-address*]

Syntax Description

ip-address	(Optional) IP address of the multicast group. Default address is 224.0.1.1.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

Use this command to allow the system to listen to multicast packets on an interface-by-interface basis.

Examples

In the following example, the system is configured to receive (listen to) NTP multicast packets on Ethernet interface 1:

```
Router(config)# interface ethernet 1
Router(config-if)# ntp multicast client
```

Related Commands

Command	Description
ntp multicast	Configures the specified interface to send NTP multicast packets.

ntp peer

To configure the software clock to synchronize a peer or to be synchronized by a peer, use the **ntp peer** command in global configuration mode. To disable this capability, use the **no** form of this command.

ntp peer *ip-address* [**version** *number*] [**key** *key-id*] [**source** *interface*] [**prefer**]

no ntp peer *ip-address*

Syntax Description

ip-address	IP address of the peer providing, or being provided, the clock synchronization.
version	(Optional) Defines the Network Time Protocol (NTP) version number.
number	(Optional) NTP version number (1 to 3).
key	(Optional) Defines the authentication key.
keyid	(Optional) Authentication key to use when sending packets to this peer.
source	(Optional) Names the interface.
interface	(Optional) Name of the interface from which to pick the IP source address.
prefer	(Optional) Makes this peer the preferred peer that provides synchronization.

Defaults

No peers are configured by default. If a peer is configured, the default NTP version number is 3, no authentication key is used, and the source IP address is taken from the outgoing interface.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command if you want to allow this machine to synchronize with the peer, or vice versa. Using the **prefer** keyword reduces switching back and forth between peers.

Tip If you are using the default version of 3 and NTP synchronization does not occur, try using NTP version 2 (NTPv2).

Examples

The following example configures a router to allow its software clock to be synchronized with the clock of the peer (or vice versa) at IP address 192.168.22.33 using NTP version 2. The source IP address is the address of Ethernet 0.

```
Router(config)# ntp peer 192.168.22.33 version 2 source ethernet 0
```

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp server	Allows the software clock to be synchronized by a time server.
ntp source	Uses a particular source address in NTP packets.

ntp refclock

To configure an external clock source for use with Network Time Protocol (NTP) services, use the **ntp refclock** command in line configuration mode. To disable support of the external time source, use the **no** form of this command.

ntp refclock {**trimble** | **telecom-solutions**} **pps** {**cts** | **ri** | **none**} [**inverted**] [**pps-offset** *number*] [**stratum** *number*] [**timestamp-offset** *number*]

no ntp refclock

Syntax Description

trimble	Enables the reference clock driver for the Trimble Palisade NTP Synchronization Kit (Cisco 7200 series routers only).
telecom-solutions	Enables the reference clock driver for a Telecom Solutions GPS device.
pps	Pulse per second (PPS) signal line. Indicate PPS pulse reference clock support. Choices are **cts**, **ri**, or **none**.
cts	Pulse per second on CTS.
ri	Pulse per second on RI.
none	No PPS signal available.
inverted	(Optional) PPS signal is inverted.
pps-offset *number*	(Optional) Offset of PPS pulse. The number is the offset (in milliseconds).
stratum *number*	(Optional) Number from 0 to 14. Indicates the NTP stratum number that the system will claim.
timestamp-offset *number*	(Optional) Offset of time stamp. The number is the offset (in milliseconds).

Defaults

This command is disabled by default.

Command Modes

Line configuration

Command History

Release	Modification
12.1	The **trimble** keyword was added to provide driver activation for a Trimble GPS time source on the Cisco 7200 series router.

Usage Guidelines

To configure a PPS signal as the source for NTP synchronization, use the following form of the **ntp refclock** command:

ntp refclock pps {**cts** | **ri**} [**inverted**] [**pps-offset** *number*] [**stratum** *number*] [**timestamp-offset** *number*]

To configure a Trimble Palisade NTP Synchronization Kit as the GPS clock source connected to the auxiliary port of a Cisco 7200 router, use the following form of the **ntp refclock** command:

ntp refclock trimble pps none [**stratum** *number*]

To configure a Telecom Solutions product as the GPS clock source, use the **ntp refclock telecom-solutions** form of the command:

ntp refclock telecom-solutions pps cts [**stratum** *number*]

Examples

The following example shows configuration of a Trimble Palisade GPS time source on a Cisco 7200 router:

```
Router(config)# ntp master
Router(config)# ntp update-calendar
Router(config)# line aux 0
Router(config-line)# ntp refclock trimble pps none
```

The following example shows configuration of a Telecom Solutions GPS time source on a Catalyst switch platform:

```
Router(config)# ntp master
Router(config)# ntp update-calendar
Router(config)# line aux 0
Router(config-line)# ntp refclock telecom-solutions pps cts stratum 1
```

Related Commands

Command	Description
show ntp associations	Displays the status of NTP associations configured for your system.

ntp server

To allow the software clock to be synchronized by a Network Time Protocol (NTP) time server, use the **ntp server** command in global configuration mode. To disable this capability, use the **no** form of this command.

ntp server *ip-address* [**version** *number*] [**key** *key-id*] [**source** *interface*] [**prefer**]

no ntp server *ip-address*

Syntax Description

ip-address	IP address of the time server providing the clock synchronization.
version	(Optional) Defines the NTP version number.
number	(Optional) NTP version number (1 to 3).
key	(Optional) Defines the authentication key.
key-id	(Optional) Authentication key to use when sending packets to this peer.
source	(Optional) Identifies the interface from which to pick the IP source address.
interface	(Optional) Name of the interface from which to pick the IP source address.
prefer	(Optional) Specifies that the server referenced in this command is preferred over other configured NTP servers.

Defaults

No peers are configured by default. If a peer is configured, the default NTP version number is 3, no authentication key is used, and the source IP address is taken from the outgoing interface.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command if you want to allow the system to synchronize with the specified server. The server will not synchronize to this machine.

Use the **prefer** keyword if you use this command multiple times, and you want to set a preferred server. Using the **prefer** keyword reduces switching back and forth between servers.

If you are using the default version of 3 and NTP synchronization does not occur, try using NTP version 2. Some NTP servers on the Internet run version 2.

Examples

The following example configures a router to allow its software clock to be synchronized with the clock by the device at IP address 172.16.22.44 using NTP version 2:

```
Router(config)# ntp server 172.16.22.44 version 2
```

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp peer	Configures the software clock to synchronize a peer or to be synchronized by a peer.
ntp source	Uses a particular source address in NTP packets.

ntp source

To use a particular source address in Network Time Protocol (NTP) packets, use the **ntp source** command in global configuration mode. To remove the specified source address, use the **no** form of this command.

ntp source *type number*

no ntp source

Syntax Description

type	Type of interface.
number	Number of the interface.

Defaults

Source address is determined by the outgoing interface.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command when you want to use a particular source IP address for all NTP packets. The address is taken from the named interface. This command is useful if the address on an interface cannot be used as the destination for reply packets. If the **source** keyword is present on an **ntp server** or **ntp peer** global configuration command, that value overrides the global value set by this command.

Examples

The following example configures a router to use the IP address of Ethernet 0 as the source address of all outgoing NTP packets:

```
Router(config)# ntp source ethernet 0
```

Related Commands

Command	Description
ntp peer	Configures the software clock to synchronize a peer or to be synchronized by a peer.
ntp server	Allows the software clock to be synchronized by a time server.

ntp trusted-key

To authenticate the identity of a system to which Network Time Protocol (NTP) will synchronize, use the **ntp trusted-key** command in global configuration mode. To disable authentication of the identity of the system, use the **no** form of this command.

ntp trusted-key *key-number*

no ntp trusted-key *key-number*

Syntax Description

key-number	Key number of authentication key to be trusted.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

If authentication is enabled, use this command to define one or more key numbers (corresponding to the keys defined with the **ntp authentication-key** command) that a peer NTP system must provide in its NTP packets, in order for this system to synchronize to it. This function provides protection against accidentally synchronizing the system to a system that is not trusted, because the other system must know the correct authentication key.

Examples

The following example configures the system to synchronize only to systems providing authentication key 42 in its NTP packets:

```
Router(config)# ntp authenticate
Router(config)# ntp authentication-key 42 md5 aNiceKey
Router(config)# ntp trusted-key 42
```

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Defines an authentication key for NTP.

ntp update-calendar

To periodically update the hardware clock (calendar) from a Network Time Protocol (NTP) time source, use the **ntp update-calendar** command in global configuration mode. To disable the periodic updates, use the **no** form of this command.

ntp update-calendar

no ntp update-calendar

Syntax Description

This command has no arguments or keywords.

Defaults

The hardware clock (calendar) is not updated.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Some platforms have a battery-powered hardware clock, referred to in the command-line interface (CLI) as the "calendar," in addition to the software based system clock. The hardware clock runs continuously, even if the router is powered off or rebooted.

If the software clock is synchronized to an outside time source via NTP, it is a good practice to periodically update the hardware clock with the time learned from NTP. Otherwise, the hardware clock will tend to gradually lose or gain time (drift), and the software clock and hardware clock may become out of synchronization with each other. The **ntp update-calendar** command will enable the hardware clock to be periodically updated with the time specified by the NTP source. The hardware clock will be updated only if NTP has synchronized to an authoritative time server.

Many lower-end routers (for example, the Cisco 2500 series or the Cisco 2600 series) do not have hardware clocks, so this command is not available on those platforms.

To force a single update of the hardware clock from the software clock, use the **clock update-calendar** EXEC command.

Examples

The following example configures the system to periodically update the hardware clock from the NTP time source:

```
Router(config)# ntp update-calendar
```

Related Commands

Command	Description
clock read-calendar	Performs a one-time update of the software clock from the hardware clock (calendar).
clock update-calendar	Performs a one-time update of the hardware clock (calendar) from the software clock.

owner

To configure the Simple Network Management Protocol (SNMP) owner of an Service Assurance Agent (SAA) operation, use the **owner** command in SAA RTR configuration mode. To return to the default value, use the **no** form of this command.

owner *text*

no owner

Syntax Description

text	Name of the SNMP owner from 0 to 255 ASCII characters. The default is none.

Defaults

No owner is specified.

Command Modes

SAA RTR configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The owner name contains one or more of the following: ASCII form of the network management station's transport address, network management station name (that is, the domain name), and network management personnel's name, location, or phone number. In some cases, the agent itself will be the owner of the operation. In these cases, the name can begin with "agent."

Examples

The following example sets the owner of operation 1 to 172.16.1.189 cwb.cisco.com John Doe RTP 555-1212:

```
Router(config)# rtr 1
Router(config-rtr)# type echo protocol ipIcmpEcho 172.16.1.176
Router(config-rtr)# owner 172.16.1.189 cwb.cisco.com John Doe RTP 555-1212
```

Related Commands

Command	Description
rtr	Enters SAA RTR configuration mode.

padding

To set the padding on a specific output character, use the **padding** command in line configuration mode. To remove padding for the specified output character, use the **no** form of this command.

padding *ascii-number count*

no padding *ascii-number*

Syntax Description

ascii-number	ACII decimal representation of the character.
count	Number of NULL bytes sent after the specified character, up to 255 padding characters in length.

Defaults

No padding

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command when the attached device is an old terminal that requires padding after certain characters (such as ones that scrolled or moved the carriage). See the "ASCII Character Set and Hex Values" appendix for a list of ASCII characters.

Examples

In the following example, the Return (decimal character 13) is padded with 25 NULL bytes on the console line:

```
Router(config)# line console
Router(config-line)# padding 13 25
```

Related Commands

Command	Description
terminal padding	Changes the character padding on a specific output character for the current session.

parity

To define generation of a parity bit, use the **parity** command in line configuration mode. To specify no parity, use the **no** form of this command.

parity {**none** | **even** | **odd** | **space** | **mark**}

no parity

Syntax Description

none	No parity. This is the default.
even	Even parity.
odd	Odd parity.
space	Space parity.
mark	Mark parity.

Defaults

No parity.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Communication protocols provided by devices such as terminals and modems will sometimes require a specific parity bit setting. Refer to the documentation for your device to determine required parity settings.

Examples

In the following example even parity is configured for line 34:

```
Router(config)# line 34
Router(config-line)# parity even
```

Related Commands

Command	Description
terminal parity	Defines the generation of the parity bit for the current for the current session and line.

parser cache

To reenable the Cisco IOS software parser cache after disabling it, use the **parser cache** command in global configuration mode. To disable the parser cache, use the **no** form of this command.

parser cache

no parser cache

Syntax Description

This command has no arguments or keywords.

Defaults

Parser cache is enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

The Parser Cache feature optimizes the parsing (translation and execution) of Cisco IOS software configuration command lines by remembering how to parse recently encountered command lines, decreasing the time required to process large configuration files.

The parser cache is enabled by default. However, if you wish to disable the parser cache, you may do so using the **no parser cache** command in global configuration mode. To reenable the parser cache after it has been disabled, use the **parser cache** command.

When the **no parser cache** is issued, the command line appears in the running configuration file. However, if the parser cache is reenabled, no command line appears in the running configuration file.

Examples

In the following example, the Cisco IOS software Parser Cache feature is disabled:

```
Router(config)# no parser cache
```

Related Commands

Command	Description
clear parser cache	Clears the parse cache entries and hit/miss statistics stored for the Parser Cache feature.
show parser statistics	Displays statistics about the last configuration file parsed and the status of the Parser Cache feature.

partition

To separate Flash memory into partitions on Class B file system platforms, use the **partition** command in global configuration mode. To undo partitioning and to restore Flash memory to one partition, use the **no** form of this command.

Cisco 1600 Series and Cisco 3600 Series Routers

partition *flash-filesystem***:** [*number-of-partitions*][*partition-size*]

no partition *flash-filesystem***:**

All Other Class B Platforms

partition flash *partitions* [*size1 size2*]

no partition flash

Syntax Description

*flash-filesystem***:**	One of the following Flash file systems, which must be followed by a colon (:). The Cisco 1600 series can only use the **flash:** keyword. • **flash:**—Internal Flash memory • **slot0:**—Flash memory card in PCMCIA slot 0 • **slot1:**—Flash memory card in PCMCIA slot 1
number-of-partitions	(Optional) Number of partitions in Flash memory.
partition-size	(Optional) Size of each partition. The number of partition size entries must be equal to the number of specified partitions.
partitions	Number of partitions in Flash memory. Can be 1 or 2.
size1	(Optional) Size of the first partition (in megabytes).
size2	(Optional) Size of the second partition (in megabytes).

Defaults

Flash memory consists of one partition.

If the partition size is not specified, partitions of equal size are created.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

For the Cisco 1600 series and Cisco 3600 series routers, to undo partitioning, use the **partition** *flash-filesystem***:1** or **no partition** *flash-filesystem***:** command. For other Class B platforms, use either the **partition flash 1** or **no partition flash** command. If there are files in a partition other than the first, you must use the **erase** *flash-filesystem:partition-number* command to erase the partition before reverting to a single partition.

When creating two partitions, you must not truncate a file or cause a file to spill over into the second partition.

Examples

The following example creates two partitions of 4 MB each in Flash memory:

```
Router(config)# partition flash 2 4 4
```

The following example divides the Flash memory card in slot 0 into two partitions, each 8 MB in size on a Cisco 3600 series router:

```
Router(config)# partition slot0: 2 8 8
```

The following example creates four partitions of equal size in the card on a Cisco 1600 series router:

```
Router(config)# partition flash: 4
```

paths-of-statistics-kept

To set the number of paths for which statistics are maintained per hour for the Service Assurance Agent (SAA) operation, use the **paths-of-statistics-kept** command in SAA RTR configuration mode. To return to the default value, use the **no** form of this command.

paths-of-statistics-kept *size*

no paths-of-statistics-kept

Syntax Description

size	Number of paths for which statistics are maintained per hour. The default is 5 paths for **type pathEcho** and 1 path for **type echo**.

Defaults

5 paths for **type pathEcho**

1 path for **type echo**

Command Modes

SAA RTR configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

A path is the route the request packet of the operation takes through the network to get to its destination. The operation may take a different path to reach its destination for each SAA operation.

When the number of paths reaches the size specified, no further path information is stored.

Examples

The following example maintains statistics for only 3 paths for operation 2:

```
Router(config)# rtr 2
Router(config-rtr)# type pathEcho protocol ipIcmpEcho 172.16.1.177
Router(config-rtr)# paths-of-statistics-kept 3
```

Related Commands

Command	Description
distributions-of-statistics-kept	Sets the number of statistic distributions kept per hop during the lifetime of the SA.
hops-of-statistics-kept	Sets the number of hops for which statistics are maintained per path for the SAA operation.
hours-of-statistics-kept	Sets the number of hours for which statistics are maintained for the SAA operation.

Command	Description
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.
statistics-distribution-interval	Sets the time interval for each statistics distribution kept for the SAA.

periodic

To specify a recurring (weekly) time range for functions that support the time-range feature, use the **periodic** command in time-range configuration mode. To remove the time limitation, use the **no** form of this command.

periodic *days-of-the-week hh:mm* **to** [*days-of-the-week*] *hh:mm*

no periodic *days-of-the-week hh:mm* **to** [*days-of-the-week*] *hh:mm*

Syntax Description

days-of-the-week	The first occurrence of this argument is the starting day or day of the week that the associated time range is in effect. The second occurrence is the ending day or day of the week the associated statement is in effect. This argument can be any single day or combinations of days: **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, and **Sunday**. Other possible values are: • **daily**—Monday through Sunday • **weekdays**—Monday through Friday • **weekend**—Saturday and Sunday If the ending days of the week are the same as the starting days of the week, they can be omitted.
hh:mm	The first occurrence of this argument is the starting hours:minutes that the associated time range is in effect. The second occurrence is the ending hours:minutes the associated statement is in effect. The hours:minutes are expressed in a 24-hour clock. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m.
to	Entry of the **to** keyword is required to complete the range "from start-time to end-time."

Defaults

No recurring time range is defined.

Command Modes

Time-range configuration (config-time-range)

Command History

Release	Modification
12.0(1)T	This command was introduced.

Usage Guidelines

For Cisco IOS Release 12.2(11)T, IP and Internetwork Packet Exchange (IPX) extended access lists are the only functions that can use time ranges. For further information on using these functions, refer to the *Cisco IOS IP Configuration Guide* and the *Cisco IOS AppleTalk and Novell IPX Configuration Guide*.

The **periodic** command is one way to specify when a time range is in effect. Another way is to specify an absolute time period with the **absolute** command. Use either of these commands after the **time-range** global configuration command, which specifies the name of the time range. Multiple **periodic** entries are allowed per **time-range** command.

If the end days-of-the-week value is the same as the start value, they can be omitted.

If a **time-range** command has both **absolute** and **periodic** values specified, then the **periodic** items are evaluated only after the **absolute start** time is reached, and are not further evaluated after the **absolute end** time is reached.

Note All time specifications are taken as local time. To ensure that the time range entries take effect at the desired times, you should synchronize the system software clock using Network Time Protocol (NTP).

Table 36 lists some typical settings for your convenience:

Table 36 Typical Examples of periodic Command Syntax

If you want:	Configure this:
Monday through Friday, 8:00 a.m. to 6:00 p.m. only	**periodic weekday 8:00 to 18:00**
Every day of the week, from 8:00 a.m. to 6:00 p.m. only	**periodic daily 8:00 to 18:00**
Every minute from Monday 8:00 a.m. to Friday 8:00 p.m.	**periodic monday 8:00 to friday 20:00**
All weekend, from Saturday morning through Sunday night	**periodic weekend 00:00 to 23:59**
Saturdays and Sundays, from noon to midnight	**periodic weekend 12:00 to 23:59**

Examples

The following example configuration denies HTTP traffic on Monday through Friday from 8:00 a.m. to 6:00 p.m.:

```
Router# show startup-config
.
.
.
time-range no-http
 periodic weekdays 8:00 to 18:00
!
ip access-list extended strict
 deny tcp any any eq http time-range no-http
!
interface ethernet 0
 ip access-group strict in
.
.
.
```

The following example configuration permits Telnet traffic on Mondays, Tuesdays, and Fridays from 9:00 a.m. to 5:00 p.m.:

```
Router# show startup-config

.
.
.
```

```
time-range testing
 periodic Monday Tuesday Friday 9:00 to 17:00
!
ip access-list extended legal
 permit tcp any any eq telnet time-range testing
!
interface ethernet 0
 ip access-group legal in
.
.
.
```

Related Commands

Command	Description
absolute	Specifies an absolute start and end time for a time range.
access-list (extended)	Defines an extended IP access list.
deny (IP)	Sets conditions under which a packet does not pass a named IP access list.
permit (IP)	Sets conditions under which a packet passes a named IP access list.
time-range	Enables time-range configuration mode and names a time range definition.

ping

To diagnose basic network connectivity on AppleTalk, ATM, Connectionless Network Service (CLNS), DECnet, IP, Novell IPX, or source-route bridging (SRB) networks, use the **ping** command in Exec mode.

ping [*protocol*] [**tag**] {*host-name* | *system-address*}

Syntax Description

protocol	(Optional) Protocol keyword, one of **appletalk**, **atm**, **clns**, **decnet**, **ipx**, or **srb**. If a specific protocol is not specified, a basic ping will be sent using IP (IPv4). For extendend options for ping over IP, see the documentation for the **ping ip** command. **Note** The **ping atm interface atm**, **ping ip**, **ping ipv6**, **ping sna**, and **ping vrf** commands are documented separately.
tag	(Optional) Specifies a tag encapsulated IP (tagIP) ping.
host-name	Host name of the system to ping. If a *host-name* or *system-address* is not specified at the command line, it will be required in the **ping** system dialog.
system-address	Address of the system to ping. If a *host-name* or *system-address* is not specified at the command line, it will be required in the **ping** system dialog.

Defaults

A basic ping operation to the specified address or host-name is performed, using IP.

Command Modes

Exec

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	The **ping sna** command was introduced.
12.1(12c)E	Support for the specification of a VRF was added for the ping command (see the command reference page for the **ping vrf** command).
12.2(2)T	Support for the IPv6 protocol was added.
12.2(13)T	The **atm** protocol keyword was added. The following keywords were removed because the Apollo Domain, Banyan VINES, and XNS protocols are no longer supported in Cisco IOS software: • **apollo** • **vines** • **xns**

Usage Guidelines

The **ping** command sends an echo request packet to an address, and then awaits a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning. For example, the **ping clns** command sends CLNS echo packets to test the reachability of a remote router over a connectionless Open System Interconnection (OSI) network.

If you enter the **ping** command without any other syntax (**ping**<cr>), the CLI will display a system dialog (the interactive dialog for ping) that prompts you for the additional syntax appropriate to the protocol you specify (See the "Examples" section).

To abnormally terminate a ping session, type the escape sequence—by default, **Ctrl-^ 6X**. You type the default by simultaneously pressing and releasing the **Ctrl**, **Shift**, and **6** keys and then pressing the **X** key.

Table 37 describes the test characters sent by the **ping** facility.

Table 37 ping Test Characters

Character	Description
!	Each exclamation point indicates receipt of a reply.
.	Each period indicates that the network server timed out while waiting for a reply.
U	A destination unreachable error protocol data unit (PDU) was received.
C	A congestion experienced packet was received.
I	User interrupted test.
?	Unknown packet type.
&	Packet lifetime exceeded.

Note Not all protocols require hosts to support pings. For some protocols, the pings are Cisco-defined and can be answered only by another Cisco router.

The availability of protocol keywords depends on what protocols are enabled on your system.

Issuing the **ping** command in User Exec mode will generally offer fewer syntax options than issuing the **ping** command in Privileged Exec mode.

For additional information on the ping command, see the "Using the Extended ping and Extended traceroute Commands" tech note, available on Cisco.com.

Examples

In the following example, a basic ping operation is performed using IP/ICMP. As all required syntax is specified at the command line, the interactive dialog for ping is not started.

```
Router# ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
cs-7204-15a#
5w1d: IP: s=10.1.1.1 (local), d=10.1.1.1 (ATM4/0), len 100, sending
5w1d: IP: s=10.1.1.1 (ATM4/0), d=10.1.1.1 (ATM4/0), len 100, rcvd 3
5w1d: IP: s=10.1.1.1 (local), d=10.1.1.1 (ATM4/0), len 100, sending
5w1d: IP: s=10.1.1.1 (ATM4/0), d=10.1.1.1 (ATM4/0), len 100, rcvd 3
```

In the following example, the interactive dialog for ping is started. The dialog options will vary based on the protocol you specify.

```
Router# ping

Protocol [ip]:
```

```
Target IP address: 192.168.7.27

Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.27, timeout is 2 seconds:
!!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/2/4 ms
```

Table 38 describes the significant prompts and output shown in this example.

Table 38 Field Descriptions for Ping Interactive Dialog

Field	Description
Protocol [ip]:	Prompts for a supported protocol. Enter **atm**, **clns**, **decnet**, **ip**, **ipv6**, **ipx**, or **srb**. Default: **ip**.
Target IP address:	Prompts for the IP address or host name of the destination node you plan to ping. If you have specified a supported protocol other than IP, enter an appropriate address for that protocol here. Default: none.
Repeat count [5]:	Number of ping packets that will be sent to the destination address. Default: 5.
Datagram size [100]:	Size of the ping packet, in bytes. Default: 100.
Timeout in seconds [2]:	Timeout interval, in seconds. Default: 2.
Extended commands [n]:	Specifies whether a series of additional commands appears.
Sweep range of sizes [n]:	Allows you to vary the sizes of the echo packets being sent. This capability is useful for determining the minimum sizes of the MTUs[1] configured on the nodes along the path to the destination address. Packet fragmentation contributing to performance problems can then be reduced.
!!!!!	Each exclamation point (!) indicates receipt of a reply. A period (.) indicates that the network server timed out while waiting for a reply. Other characters may appear in the ping output display, depending on the protocol type.
Success rate is 100 percent	Percentage of packets successfully echoed back to the router. Anything less than 80 percent is usually considered problematic.
round-trip min/avg/max = 1/2/4 ms	Round-trip travel time intervals for the protocol echo packets, including minimum/average/maximum (in milliseconds).

1. MTU = maximum transmission unit

The following example verifies connectivity to the neighboring ATM device for the ATM PVC with the virtual path identifier (VPI)/virtual channel identifier (VCI) value 0/16:

```
Router# ping

Protocol [ip]:atm
```

```
ATM Interface:atm1/0
VPI value [0]:
VCI value [1]:16
Loopback - End(0), Segment(1) [0]:1
Repeat Count [5]:
Timeout [2]:
Type escape sequence to abort.
Sending 5, 53-byte segment OAM echoes, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Table 39 describes the prompts and output shown when ATM is specified.

Table 39 Field Descriptions for the Ping Interactive Dialog for ATM

Prompt	Description
ATM Interface:	Prompt for the ATM interface ID.
VPI value [0]:	Prompt for the virtual path identifier. Default: 0.
VCI value [1]:	Prompt for the virtual channel identifier. Default:1.
Loopback - End(0), Segment(1) [0]:	Prompt to specify end loopback, which verifies end-to-end PVC integrity, or segment loopback, which verifies PVC integrity to the neighboring ATM device. Default: segment loopback.
Repeat Count [5]:	Number of ping packets that will be sent to the destination address. Default: 5.
Timeout [2]:	Timeout interval. Default: 2 (seconds).
!!!!!	Each exclamation point (!) indicates receipt of a reply. A period (.) indicates that the network server timed out while waiting for a reply. Other characters may appear in the ping output display, depending on the protocol type.
Success rate is 100 percent	Percentage of packets successfully echoed back to the router. Anything less than 80 percent is usually considered problematic.
round-trip min/avg/max = 1/1/1 ms	Round-trip travel time intervals for the protocol echo packets, including minimum/average/maximum (in milliseconds).

Related Commands

Command	Description
ping atm interface atm	Tests the connectivity of a specific PVC.
ping ip	Tests the connection to a remote host on the network using IPv4.
ping ipv6	Tests the connection to a remote host on the network using IPv6.
ping sna	Tests network integrity and timing characteristics over an SNA Switching network.
ping vrf	Tests a connection in the context of a specific VPN (VRF).

ping ip

To test network connectivity on IP networks, use the **ping ip** command in privileged EXEC mode.

ping ip {*host-name* | *system-address*} [**data** [*hex-data-pattern*] | **df-bit** | **repeat** [*repeat-count*] | **size** [*datagram-size*] [**source** {*source-address* | *source-interface*}] [**timeout** *seconds*] [**validate**]

Syntax Description

host-name	Host name of the system to ping.
system-address	Address of the system to ping.
data *hex-data-pattern*	(Optional) Specifies the data pattern. Range is from 0 to FFFF.
df-bit	(Optional) Enables the "do-not-fragment" bit in the IP header.
repeat *repeat-count*	(Optional) Specifies the number of pings sent. The range is from 1 to 2147483647. The default is 5.
size	(Optional) Specifies the datagram size. Datagram size is the number of bytes in each ping.
datagram-size	(Optional) Range is from 40 to 18024.
source	(Optional) Specifies the source address or source interface.
source-address	(Optional) IP address to use as the source in the ping packets.
source-interface	(Optional) Name of the interface from which the ping should be sent, and the Interface ID (slot/port/number). Interface name keywords include the following: • **async** (Asynchronous Interface) • **bvi** (Bridge-Group Virtual Interface) • **ctunnel** • **dialer** • **ethernet** • **fastEthernet** • **lex** • **loopback** • **multilink** (Multilink-group interface) • **null** • **port-channel** (Ethernet channel of interfaces) • **tunnel** • **vif** (PGM Multicast Host interface) • **virtual-template** • **virtual-tokenring** • **xtagatm** (Extended Tag ATM interface) The availability of these keywords depends on your system hardware.
timeout *seconds*	(Optional) Specifies the timeout interval in seconds. The default is 2 seconds. Range is from 0 to 3600.
validate	(Optional) Validates the reply data.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0	The **data**, **df-bit**, **repeat**, **size**, **source**, **timeout**, and **validate** keywords were added.

Usage Guidelines

The **ping** command sends an echo request packet to an address, then awaits a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

To abnormally terminate a ping session, type the escape sequence—by default, **Ctrl-^ X**. You type the default by simultaneously pressing and releasing the **Ctrl**, **Shift**, and **6** keys, and then pressing the **X** key.

Table 40 describes the test characters that the ping facility sends.

Table 40 ping Test Characters

Character	Description
!	Each exclamation point indicates receipt of a reply.
.	Each period indicates that the network server timed out while waiting for a reply.
U	A destination unreachable error protocol data unit (PDU) was received.
C	A congestion experienced packet was received.
I	User interrupted test.
?	Unknown packet type.
&	Packet lifetime exceeded.

Note Not all protocols require hosts to support pings. For some protocols, the pings are Cisco-defined and are only answered by another Cisco router.

Examples

After you enter the **ping** command in privileged mode, the system prompts for one of the following keywords: **apollo**, **appletalk**, **clns**, **decnet**, **ip**, **novell**, **vines**, or **xns**. The default protocol is IP.

If you enter a host name or address on the same line as the **ping** command, the default action is taken as appropriate for the protocol type of that name or address.

The optional **data**, **df-bit**, **repeat**, **size**, **source**, **timeout**, and **validate** keywords can be used to avoid extended **ping** command output. You can use as many of these keywords as you need, and you can use them in any order after the *host-name* or *system-address* arguments.

Although the precise dialog varies somewhat from protocol to protocol, all are similar to the ping session using default values shown in the following output:

```
Router# ping

Protocol [ip]:
Target IP address: 192.168.7.27
```

```
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.27, timeout is 2 seconds:
!!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/2/4 ms
```

Table 41 describes the default **ping** fields shown in the display.

Table 41 ping Field Descriptions

Field	Description
Protocol [ip]:	Prompts for a supported protocol. Enter **appletalk**, **clns**, **ip**, **novell**, **apollo**, **vines**, **decnet**, or **xns**. The default is IP.
Target IP address:	Prompts for the IP address or host name of the destination node you plan to ping. If you have specified a supported protocol other than IP, enter an appropriate address for that protocol here. The default is none.
Repeat count [5]:	Prompts for the number of ping packets that will be sent to the destination address. The default is 5 packets.
Datagram size [100]:	Prompts for the size of the ping packet (in bytes). The default is 100 bytes.
Timeout in seconds [2]:	Prompts for the timeout interval. The default is 2 seconds.
Extended commands [n]:	Specifies whether a series of additional commands appears.
Sweep range of sizes [n]:	Allows you to vary the sizes of the echo packets being sent. This capability is useful for determining the minimum sizes of the MTUs configured on the nodes along the path to the destination address. Packet fragmentation contributing to performance problems can then be reduced.
!!!!!	Each exclamation point (!) indicates receipt of a reply. A period (.) indicates that the network server timed out while waiting for a reply. Other characters may appear in the ping output display, depending on the protocol type.
Success rate is 100 percent	Indicates the percentage of packets successfully echoed back to the router. Anything less than 80 percent is usually considered problematic.
round-trip min/avg/max = 1/2/4 ms	Indicates the round-trip travel time intervals for the protocol echo packets, including minimum/average/maximum (in milliseconds).

Related Commands

Command	Description
ping ipv6	Tests the connection to a remote host on the network using IPv6.
ping vrf	Tests a connection in the context of a specific VPN (VRF).

ping vrf

To test a connection in the context of a specific VPN connection, use the **ping vrf** command in Exec mode.

ping vrf *vrf-name* [**tag**] [*connection*] *target-address* [*connection-options*]

Syntax Description

vrf-name	The name of the VPN (VRF context).
tag	(Optional) Specifies a tag encapsulated IP (tagIP) ping.
connection	(Optional) Connection options include **atm**, **clns**, **decnet**, **ip**, **ipv6**, **ipx**, **sna**, or **srb**. The default is **ip**.
target-address	The destination ID for the ping operation. Usually, this is the IP-address of the host. For example, the target for an IP ping in a VRF context would be the IP address or domain name of the target host. • If the target address is not specified, the CLI will enter the interactive dialog for ping.
connection-options	Each connection type may have its own set of connection options. For example, connection options for IP include **source**, **df-bit**, and **timeout**. See the appropriate **ping** command documentation for details.

Defaults

The default connection type for ping is IP (specifically, IPv4).

Command Modes

User Exec

Privileged Exec

Command History

Release	Modification
12.1(12c)E, 12.2	This command was introduced.

Usage Guidelines

A VPN routing/forwarding (VRF) instance is used to identify a VPN. To check if a configured VRF is working, you can use the **ping vrf** command.

When attempting to ping from a provider edge (PE) router to a customer edge (CE) router, or from a PE router to PE router, the standard **ping** command will not usually work. The **ping vrf** command allows you to ping the IP addresses of LAN interfaces on CE routers.

If you are on a PE router, be sure to indicate the specific VRF (VPN) name, as shown in the "Examples" section.

If all required information is not provided at the command line, the system will enter the interactive dialog (extended mode) for ping.

Examples

In the following example, the target host in the domain 209.165.201.1 is pinged (using IP/ICMP) in the context of the "Customer_A" VPN connection.

```
Router# ping vrf Customer_A 209.165.201.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 176/264/576 ms
```

Pressing the Enter key before providing all of the required options will begin the interactive dialog for ping. In the following example, the interactive dialog is started after the "ip" protocol is specified, but no address is given:

```
Router# ping vrf Customer_B ip
Target IP address: 209.165.200.225
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]: Record
Number of hops [ 9 ]:
Loose, Strict, Record, Timestamp, Verbose[RV]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2 seconds:
Packet has IP options:  Total option bytes= 39, padded length=40
 Record route: <*>
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
 .
 .
 .
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

The following example shows the various options for IP in the **ping vrf** command:

```
Router# show parser dump exec | include ping vrf
1 ping vrf <string>
1 ping vrf <string> ip <string>
1 ping vrf <string> ip (interactive)
1 ping vrf <string> ip <string>
1 ping vrf <string> ip <string> source <address>
1 ping vrf <string> ip <string> source <interface>
1 ping vrf <string> ip <string> repeat <1-2147483647>
1 ping vrf <string> ip <string> size Number
1 ping vrf <string> ip <string> df-bit
1 ping vrf <string> ip <string> validate
1 ping vrf <string> ip <string> data <0-65535>
1 ping vrf <string> ip <string> timeout <0-3600>
1 ping vrf <string> ip <string> verbose
1 ping vrf <string> ip <string> data <0-65535>
1 ping vrf <string> ip <string> timeout <0-3600>
```

```
1 ping vrf <string> tag
1 ping vrf <string> atm
1 ping vrf <string> ipv6
1 ping vrf <string> appletalk
1 ping vrf <string> decnet
1 ping vrf <string> clns
1 ping vrf <string> ipx
1 ping vrf <string> sna
1 ping vrf <string> srb
```

Related Commands

Command	Description
ping	Diagnoses basic network connectivity to a specific host.
ping atm interface atm	Tests the connectivity of a specific PVC.
ping ip	Tests the connection to a remote host on the network using IPv4.
ping ipv6	Tests the connection to a remote host on the network using IPv6.
ping sna	Tests network integrity and timing characteristics over an SNA Switching network.

policy-list

To associate a policy list with a Command Scheduler occurrence, use the **policy-list** command in kron-occurrence configuration mode. To delete a policy list from the Command Scheduler occurrence, use the **no** form of this command.

policy-list *list-name*

no policy-list *list-name*

Syntax Description

list-name	Name of policy list. If the *list-name* is new, a policy list structure will be created. If the *list-name* is not new, the existing policy list will be edited.

Defaults

No policy list is associated.

Command Modes

Kron-occurrence configuration (config-kron-occurrence)

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use the **policy-list** command with the **kron occurrence** command to schedule one or more policy lists to run at the same time or interval. Use the **kron policy-list** command in conjunction with the **cli** command to create a Command Scheduler policy list containing EXEC command line interface (CLI) commands to be scheduled to run on the router at a specified time.

The Command Scheduler process is useful to automate the running of EXEC commands at recurring intervals, and can it be used in remote routers to minimize manual intervention.

Examples

The following example shows how to create a Command Scheduler occurrence named may and associate a policy list named sales-may with the occurrence:

```
Router(config)# kron occurrence may at 6:30 may 20 oneshot
Router(config-kron-occurrence)# policy-list sales-may
```

Related Commands

Command	Description
cli	Specifies EXEC CLI commands within a Command Scheduler policy list.
kron occurrence	Specifies schedule parameters for a Command Scheduler occurrence and enters kron-occurrence configuration mode.
kron policy-list	Specifies a name for a Command Scheduler policy and enters kron-policy configuration mode.

printer

To configure a printer and assign a server tty line (or lines) to it, use the **printer** command in global configuration mode. To disable printing on a tty line, use the **no** form of this command.

printer *printer-name* {**line** *number* | **rotary** *number*} [**newline-convert** | **formfeed**]

no printer

Syntax Description

printer-name	Printer name.
line *number*	Assigns a tty line to the printer.
rotary *number*	Assigns a rotary group of tty lines to the printer.
newline-convert	(Optional) Converts newline (linefeed) characters to a two-character sequence "carriage-return, linefeed" (CR+LF).
formfeed	(Optional) Causes the Cisco IOS software to send a form-feed character (ASCII 0x0C) to the printer tty line immediately following each print job received from the network.

Defaults

No printers are defined by default.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This command enables you to configure a printer for operations and assign either a single tty line or a group of tty lines to it. To make multiple printers available through the same printer name, specify the number of a rotary group.

In addition to configuring the printer with the **printer** command, you must modify the file /etc/printcap on your UNIX system to include the definition of the remote printer in the Cisco IOS software. Refer to the *Cisco IOS Configuration Fundamentals Configuration Guide* for additional information.

Use the optional **newline-convert** keyword in UNIX environments that cannot handle single-character line terminators. This converts newline characters to a carriage-return, linefeed sequence. Use the **formfeed** keyword when using the line printer daemon (lpd) protocol to print and your system is unable to separate individual output jobs with a form feed (page eject). You can enter the **newline-convert** and **formfeed** keywords together and in any order.

Examples

In the following example a printer named printer1 is configured and output is assigned to tty line 4:

```
Router(config)# printer printer1 line 4
```

Related Commands

Command	Description
clear line	Returns a terminal line to idle state.

private

To save user EXEC command changes between terminal sessions, use the **private** command in line configuration mode. To restore the default condition, use the **no** form of this command.

private

no private

Syntax Description

This command has no arguments or keywords.

Defaults

User-set configuration options are cleared with the **exit** EXEC command or when the interval set with the **exec-timeout** line configuration command has passed.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command ensures that the terminal parameters set by the user remain in effect between terminal sessions. This behavior is desirable for terminals in private offices.

Examples

In the following example, line 15 (in this example, vty 1) is configured to keep all user-supplied settings at system restarts:

```
Router(config)# line 15
Router(config-line)# private
```

Related Commands

Command	Description
exec-timeout	Sets the interval that the EXEC command interpreter waits until user input is detected.
exit	Exits any configuration mode, or closes an active terminal session and terminates the EXEC.

process-max-time

To configure the amount of time after which a process should voluntarily yield to another process, use the **process-max-time** command in global configuration mode. To reset this value to the system default, use the **no** form of this command.

process-max-time *milliseconds*

no process-max-time *milliseconds*

Syntax Description

milliseconds	Maximum duration (in milliseconds) that a process can run before suspension. The range is from 20to 200 milliseconds.

Defaults

The default maximum process time is 200 milliseconds.

Command Modes

Global configuration

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

Lowering the maximum time a process can run is useful in some circumstances to ensure equitable division of CPU time among different tasks.

Only use this command if recommended to do so by the Cisco Technical Assistance Center (TAC).

Examples

The following example limits the duration that a process will run to 100 milliseconds:

```
Router(config)# process-max-time 100
```

prompt

To customize the CLI prompt, use the **prompt** command in global configuration mode. To revert to the default prompt, use the **no** form of this command.

prompt *string*

no prompt [*string*]

Syntax Description

string	Text that will be displayed on screen as the CLI prompt, including any desired prompt variables.

Defaults

The default prompt is either `Router` or the name defined with the **hostname** global configuration command, followed by an angle bracket (>) for user EXEC mode or a pound sign (#) for privileged EXEC mode.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

You can include customized variables when specifying the prompt. All prompt variables are preceded by a percent sign (%). Table 42 lists the available prompt variables.

Table 42 Custom Prompt Variables

Prompt Variable	Interpretation
%h	Host name. This is either *Router* or the name defined with the **hostname** global configuration command.
%n	Physical terminal line (tty) number of the EXEC user.
%p	Prompt character itself. It is either an angle bracket (>) for user EXEC mode or a pound sign (#) for privileged EXEC mode.
%s	Space.
%t	Tab.
%%	Percent sign (%)

Issuing the **prompt %h** command has the same effect as issuing the **no prompt** command.

Examples

The following example changes the EXEC prompt to include the tty number, followed by the name and a space:

```
Router(config)# prompt TTY%n@%h%s%p
```

The following are examples of user and privileged EXEC prompts that result from the previous command:

```
TTY17@Router1 > enable
TTY17@Router1 #
```

Related Commands

Command	Description
hostname	Specifies or modifies the host name for the network server.

pwd

To show the current setting of the **cd** command, use the **pwd** command in EXEC mode.

pwd

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC

Priviledged EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Use the **pwd** command to show which directory or file system is specified as the default by the **cd** command. For all EXEC commands that have an optional *filesystem* argument, the system uses the file system specified by the **cd** command when you omit the optional *filesystem* argument.

For example, the **dir** command contains an optional *filesystem* argument and displays a list of files on a particular file system. When you omit this *filesystem* argument, the system shows a list of the files on the file system specified by the **cd** command.

Examples

The following example shows that the present working file system specified by the **cd** command is slot 0:

```
Router> pwd
slot0:/
```

The following example uses the **cd** command to change the present file system to slot 1 and then uses the **pwd** command to display that present working file system:

```
Router> cd slot1:
Router> pwd
slot1:/
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
dir	Displays a list of files on a file system.

refuse-message

To define and enable a line-in-use message, use the **refuse-message** command in line configuration mode. To disable the message, use the **no** form of this command.

refuse-message *d message d*

no refuse-message

Syntax Description

d	Delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the message.
message	Message text.

Defaults

Disabled (no line-in-use message is displayed).

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character. You cannot use the delimiting character within the text of the message.

When you define a message using this command, the Cisco IOS software performs the following steps:

1. Accepts the connection.
2. Prints the custom message.
3. Clears the connection.

Examples

In the following example, line 5 is configured with a line-in-use message, and the user is instructed to try again later:

```
line 5
refuse-message  /The dial-out modem is currently in use.

Please try again later./
```

reload

To reload the operating system, use the **reload** command in EXEC mode.

reload [*text* | **in** [*hh***:**]*mm* [*text*] | **at** *hh***:***mm* [*month day* | *day month*] [*text*] | **cancel**]

Syntax Description

text	(Optional) Reason for the reload, 1 to 255 characters long.
in [*hh***:**]*mm*	(Optional) Schedule a reload of the software to take effect in the specified minutes or hours and minutes. The reload must take place within approximately 24 days.
at *hh***:***mm*	(Optional) Schedule a reload of the software to take place at the specified time (using a 24-hour clock). If you specify the month and day, the reload is scheduled to take place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within approximately 24 days.
month	(Optional) Name of the month, any number of characters in a unique string.
day	(Optional) Number of the day in the range from 1 to 31.
cancel	(Optional) Cancel a scheduled reload.

Command Modes

User EXEC

Priviledged EXEC

Command History

Release	Modification
10.0	The command was introduced.

Usage Guidelines

The **reload** command halts the system. If the system is set to restart on error, it reboots itself. Use the **reload** command after configuration information is entered into a file and saved to the startup configuration.

You cannot reload from a virtual terminal if the system is not set up for automatic booting. This prevents the system from dropping to the ROM monitor and thereby taking the system out of the remote user's control.

If you modify your configuration file, the system prompts you to save the configuration. During a save operation, the system asks you if you want to proceed with the save if the CONFIG_FILE variable points to a startup configuration file that no longer exists. If you say "yes" in this situation, the system goes to setup mode upon reload.

When you schedule a reload to occur at a later time, it must take place within approximately 24 days.

The **at** keyword can be used only if the system clock has be set on the router (either through NTP, the hardware calendar, or manually). The time is relative to the configured time zone on the router. To schedule reloads across several routers to occur simultaneously, the time on each router must be synchronized with NTP.

To display information about a scheduled reload, use the **show reload** EXEC command.

Examples

The following example immediately reloads the software on the router:

```
Router# reload
```

The following example reloads the software on the router in 10 minutes:

```
Router# reload in 10

Router# Reload scheduled for 11:57:08 PDT Fri Apr 21 1996 (in 10 minutes)
Proceed with reload? [confirm]
Router#
```

The following example reloads the software on the router at 1:00 p.m. today:

```
Router# reload at 13:00

Router# Reload scheduled for 13:00:00 PDT Fri Apr 21 1996 (in 1 hour and 2 minutes)
Proceed with reload? [confirm]
Router#
```

The following example reloads the software on the router on April 20 at 2:00 a.m.:

```
Router# reload at 02:00 apr 20

Router# Reload scheduled for 02:00:00 PDT Sat Apr 20 1996 (in 38 hours and 9 minutes)
Proceed with reload? [confirm]
Router#
```

The following example cancels a pending reload:

```
Router# reload cancel

%Reload cancelled.
```

Related Commands

Command	Description
copy system:running-config nvram:startup-config	Copies any file from a source to a destination.
show reload	Displays the reload status on the router.

rename

To rename a file in a Class C Flash file system, use the **rename** command in EXEC mode.

rename *url1 url2*

Syntax Description

url1	The original path and filename.
url2	The new path and filename.

Command Modes

User EXEC

Priviledged EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.

Usage Guidelines

This command is valid only on Class C Flash file systems.

Examples

In the following example, the file named Karen.1 is renamed test:

```
Router# dir

Directory of disk0:/Karen.dir/

  0  -rw-           0   Jan 21 1998 09:51:29  Karen.1
  0  -rw-           0   Jan 21 1998 09:51:29  Karen.2
  0  -rw-           0   Jan 21 1998 09:51:29  Karen.3
  0  -rw-           0   Jan 21 1998 09:51:31  Karen.4
243  -rw-         165   Jan 21 1998 09:53:17  Karen.cur

340492288 bytes total (328400896 bytes free)

Router# rename disk0:Karen.dir/Karen.1 disk0:Karen.dir/test
Router# dir

Directory of disk0:/Karen.dir/

  0  -rw-           0   Jan 21 1998 09:51:29  Karen.2
  0  -rw-           0   Jan 21 1998 09:51:29  Karen.3
  0  -rw-           0   Jan 21 1998 09:51:31  Karen.4
243  -rw-         165   Jan 21 1998 09:53:17  Karen.cur
  0  -rw-           0   Apr 24 1998 09:49:19  test

340492288 bytes total (328384512 bytes free)
```

request-data-size

To set the protocol data size in the payload of the Service Assurance Agent (SAA) operation's request packet, use the **request-data-size** command in SAA RTR configuration mode. To return to the default value, use the **no** form of this command.

request-data-size *bytes*

no request-data-size

Syntax Description

bytes	Size of the protocol data in the payload of the request packet of the operation. Range is 0 to the maximum of the protocol. The default is 1 byte.

Defaults

1 byte

Command Modes

SAA RTR configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

When the protocol name has the suffix "appl," the packet uses both a request and respond data size (see the **response-data-size** SAA RTR configuration command), and the data size is 12 bytes smaller than the normal payload size (this 12 bytes is the ARR Header used to control send and data response sizes).

Examples

The following example sets the request packet size to 40 bytes for operation 3:

```
Router(config)# rtr 3
Router(config-rtr)# type echo protocol snalu0echoappl cwbc0a
Router(config-rtr)# request-data-size 40
```

Related Commands

Command	Description
response-data-size	Sets the protocol data size in the payload of the SAA operation's response packet.
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.

response-data-size

To set the protocol data size in the payload of an Service Assurance Agent (SAA) operation's response packet, use the **response-data-size** command in SAA RTR configuration mode. To return to the default value, use the **no** form of this command.

response-data-size *bytes*

no response-data-size

Syntax Description

bytes	Size of the protocol data in the payload in the operation's response packet. For "appl" protocols, the default is 0 bytes. For all others, the default is the same value as the **request-data-size**.

Defaults

0 bytes

Command Modes

SAA RTR configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The **response-data-size** command is only applicable for the following operations:

- type echo protocol snaLU0EchoAppl
- type echo protocol snaLU2EchoAppl
- type pathEcho protocol snaLU0EchoAppl
- type pathEcho protocol snaLU2EchoAppl

Note that these protocols are defined with the **type** command that end in "appl" (for example, **snalu0echoappl**). When the protocol ends in "appl," the response data size is 12 bytes smaller than normal payload size.

Examples

The following example configures the response packet size of snaLU0 Echo operation 3 to 1440 bytes:

```
Router(config)# rtr 3
Router(config-rtr)# type echo protocol snalu0echoappl cwbc0a
Router(config-rtr)# response-data-size 1440
```

Related Commands

Command	Description
request-data-size	Sets the protocol data size in the payload of the SAA operation's request packet.
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.

rmdir

To remove an existing directory in a Class C Flash file system, use the **rmdir** command in EXEC mode.

rmdir *directory*

Syntax Description

directory	Directory to delete.

Command Modes

User EXEC

Priviledged EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.

Usage Guidelines

This command is valid only on Class C Flash file systems.

Examples

The following example deletes the directory named newdir:

```
Router# dir

Directory of flash:

  2  drwx           0   Mar 13 1993 13:16:21  newdir

8128000 bytes total (8126976 bytes free)
Router# rmdir newdir
Rmdir file name [newdir]?
Delete flash:newdir? [confirm]
Removed dir flash:newdir
Router# dir
Directory of flash:

No files in directory

8128000 bytes total (8126976 bytes free)
```

Related Commands

Command	Description
dir	Displays a list of files on a file system.
mkdir	Creates a new directory in a Class C Flash file system.

rmon

To enable Remote Monitoring (RMON) on an Ethernet interface, use the **rmon** command in interface configuration mode. To disable RMON on the interface, use the **no** form of this command.

rmon {**native** | **promiscuous**}

no rmon

Syntax Description

native	Enables RMON on the Ethernet interface. In native mode, the router processes only packets destined for this interface.
promiscuous	Enables RMON on the Ethernet interface. In promiscuous mode, the router examines every packet.

Defaults

RMON is disabled on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command enables RMON on Ethernet interfaces. A generic RMON console application is recommended in order to use the RMON network management capabilities. SNMP must also be configured. RMON provides visibility of individual nodal activity and allows you to monitor all nodes and their interaction on a LAN segment. When the **rmon** command is issued, the router automatically installs an Ethernet statistics study for the associated interface.

Note RMON can be very data and processor intensive. Users should measure usage effects to ensure that router performance is not degraded and to minimize excessive management traffic overhead. Native mode is less intensive than promiscuous mode.

All Cisco IOS software feature sets support RMON alarm and event groups. Additional RMON groups are supported in certain feature sets. Refer to the Release Notes for feature set descriptions. As a security precaution, support for the packet capture group allows capture of packet header information only; data payloads are not captured.

The RMON MIB is described in RFC 1757.

Examples

The following example enables RMON on Ethernet interface 0 and allows the router to examine only packets destined for the interface:

```
interface ethernet 0
 rmon native
```

Related Commands

Command	Description
rmon alarm	Sets an alarm on any MIB object.
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.
rmon queuesize	Changes the size of the queue that holds packets for analysis by the RMON process.
show rmon	Displays the current RMON agent status on the router.

rmon alarm

To set an alarm on any MIB object, use the **rmon alarm** command in global configuration mode. To disable the alarm, use the **no** form of this command.

rmon alarm *number variable interval* {**delta** | **absolute**} **rising-threshold** *value* [*event-number*] **falling**-threshold *value* [*event-number*] [**owner** *string*]

no rmon alarm *number*

Syntax Description

number	Alarm number, which is identical to the *alarmIndex* in the alarmTable in the Remote Monitoring (RMON) MIB.
variable	MIB object to monitor, which translates into the *alarmVariable* used in the alarmTable of the RMON MIB.
interval	Time in seconds the alarm monitors the MIB variable, which is identical to the *alarmInterval* used in the alarmTable of the RMON MIB.
delta	Tests the change between MIB variables, which affects the *alarmSampleType* in the alarmTable of the RMON MIB.
absolute	Tests each MIB variable directly, which affects the *alarmSampleType* in the alarmTable of the RMON MIB.
rising-threshold *value*	Value at which the alarm is triggered.
event-number	(Optional) Event number to trigger when the rising or falling threshold exceeds its limit. This value is identical to the alarmRisingEventIndex or the alarmFallingEventIndex in the alarmTable of the RMON MIB.
falling-threshold *value*	Value at which the alarm is reset.
owner *string*	(Optional) Specifies an owner for the alarm, which is identical to the *alarmOwner* in the alarmTable of the RMON MIB.

Defaults

No alarms configured

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The MIB object must be specified as a dotted decimal value after the entry sequence (for example, ifEntry.10.1). You cannot specify the variable name and the instance (for example, ifInOctets.1) or the entire dotted decimal notation. The variable must be of the form *entry.integer.instance*.

To disable the RMON alarms, you must use the **no** form of the command on each configured alarm. For example, enter **no rmon alarm 1**, where the 1 identifies which alarm is to be removed.

See RFC 1757 for more information about the RMON alarm group.

Examples

The following example configures an RMON alarm using the **rmon alarm** command:

```
rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1 falling-threshold 0
     owner jjohnson
```

This example configures RMON alarm number 10. The alarm monitors the MIB variable *ifEntry.20.1* once every 20 seconds until the alarm is disabled, and checks the change in the variable's rise or fall. If the *ifEntry.20.1* value shows a MIB counter increase of 15 or more, such as from 100000 to 100015, the alarm is triggered. The alarm in turn triggers event number 1, which is configured with the **rmon event** command. Possible events include a log entry or a SNMP trap. If the *ifEntry.20.1* value changes by 0 (falling-threshold 0), the alarm is reset and can be triggered again.

Related Commands

Command	Description
rmon	Enables Remote Network Monitoring (RMON) on an Ethernet interface
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.
show rmon	Displays the current RMON agent status on the router.

rmon capture-userdata

To disable the packet zeroing feature that initializes the user payload portion of each Remote Monitoring (RMON) MIB packet, use the **rmon capture-userdata** command in global configuration mode. To enable packet zeroing, use the **no** form of this command.

rmon capture-userdata

no rmon capture-userdata

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use the **show rmon matrix** command to display RMON statistics.

Examples

The following command disables the packet zeroing feature:

```
Router(config)# rmon capture-userdata
```

Related Commands

Command	Description
rmon collection matrix	Enables a RMON MIB matrix group of statistics on an interface.

rmon collection history

To enable Remote Monitoring (RMON) history gathering on an interface, use the **rmon collection history** command in interface configuration mode. To disable the history gathering on an interface, use the **no** form of this command.

rmon collection history controlEntry *integer* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]

no rmon collection history controlEntry *integer* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]

Syntax Description

controlEntry	Specifies the RMON group of statistics using a value.
integer	A value from 1 to 65535 that identifies the RMON group of statistics and matches the index value returned for Simple Network Management Protocol (SNMP) requests.
owner	(Optional) Specifies the name of the owner of the RMON group of statistics.
ownername	(Optional) Records the name of the owner of the RMON group of statistics.
buckets *bucket-number*	(Optional) Specifies the maximum number of buckets desired for the RMON collection history group of statistics.
interval *seconds*	(Optional) Specifies the number of seconds history should be gathered in a single bucket. When the interval ends, history is collected into a new bucket.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use the **show rmon capture** and **show rmon matrix** commands to display RMON statistics.

Examples

The following command enables an RMON MIB collection history group of statistics with an ID number of 20 and an owner as john:

```
Router(config-if)# rmon collection history controlEntry 20 owner john
```

Related Commands

Command	Description
show rmon capture	Displays the contents of the RMON history table.
show rmon matrix	Displays the RMON MIB matrix table.

rmon collection host

To enable a Remote Monitoring (RMON) MIB host collection group of statistics on the interface, use the **rmon collection host** command in interface configuration mode. To remove the specified RMON host collection, use the **no** form of the command.

rmon collection host controlEntry *integer* [**owner** *ownername*]

no rmon collection host controlEntry *integer* [**owner** *ownername*]

Syntax Description

controlEntry *integer*	Specifies an identification number for the RMON group of statistics. The integer can be any number in the range from 1 to 65535.
owner *ownername*	(Optional) Specifies the name of the owner of the RMON group of statistics.

Defaults

No RMON host collection is specified.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use the **show rmon hosts** and **show rmon matrix** commands to display RMON statistics.

Examples

The following command enables an RMON collection host group of statistics with an ID number of 20, and specifies john as the owner:

```
Router(config-if)# rmon collection host controlEntry 20 owner john
```

Related Commands

Command	Description
show rmon hosts	Displays the RMON MIB hosts table.
show rmon matrix	Displays the RMON MIB matrix table.

rmon collection matrix

To enable a Remote Monitoring (RMON) MIB matrix group of statistics on an interface, use the **rmon collection matrix** command in interface configuration mode. To remove a specified RMON matrix group of statistics, use the **no** form of the command.

rmon collection matrix controlEntry *integer* [**owner** *ownername*]

no rmon collection matrix controlEntry *integer* [**owner** *ownername*]

Syntax Description

controlEntry *integer*	Specifies an identification number for the RMON matrix group of statistics. The integer can be any number in the range from 1 to 65535.
owner *ownername*	(Optional) Specifies the name of the owner of the RMON matrix group of statistics.

Defaults

No RMON matrix group of statistics is specified.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use the **show rmon matrix** command to display RMON statistics.

Examples

The following command enables the RMON collection matrix group of statistics with an ID number of 25, and specifies john as the owner:

```
Router(config-if)# rmon collection matrix controlEntry 25 owner john
```

Related Commands

Command	Description
show rmon matrix	Displays the RMON MIB matrix table.

rmon collection rmon1

To enable all possible autoconfigurable Remote Monitoring (RMON) MIB statistic collections on the interface, use the **rmon collection rmon1** command in interface configuration mode. To disable these statistic collections on the interface, use the **no** form of the command.

rmon collection rmon1 controlEntry *integer* [**owner** *ownername*]

no rmon collection rmon1 controlEntry *integer* [**owner** *ownername*]

Syntax Description

controlEntry *integer*	Specifies an identification number for the RMON group of statistics. The integer can be any number in the range from 1 to 65535.
owner *ownername*	(Optional) Specifies the name of the owner of the RMON group of statistics.

Defaults

Disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use the **show rmon matrix** command to display RMON statistics.

Examples

The following command enables the RMON collection rmon1 group of statistics with an ID number of 30, and specifies “john” as the owner:

```
Router(config-if)# rmon collection rmon1 controlEntry 30 owner john
```

Related Commands

Command	Description
show rmon matrix	Displays the RMON MIB matrix table.

rmon event

To add or remove an event in the RMON event table that is associated with an RMON event number, use the **rmon event** command in global configuration mode. To disable RMON on the interface, use the **no** form of this command.

rmon event *number* [**log**] [**trap** *community*] [**description** *string*] [**owner** *string*]

no rmon event *number*

Syntax Description

number	Assigned event number, which is identical to the eventIndex in the eventTable in the RMON MIB.
log	(Optional) Generates an RMON log entry when the event is triggered and sets the *eventType* in the RMON MIB to *log* or *log-and-trap*.
trap *community*	(Optional) SNMP community string used for this trap. Configures the setting of the *eventType* in the RMON MIB for this row as either *snmp-trap* or *log-and-trap*. This value is identical to the *eventCommunityValue* in the eventTable in the RMON MIB.
description *string*	(Optional) Specifies a description of the event, which is identical to the event description in the eventTable of the RMON MIB.
owner *string*	(Optional) Owner of this event, which is identical to the *eventOwner* in the eventTable of the RMON MIB.

Defaults

No events are configured.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command applies only to the Cisco 2500 series and Cisco AS5200 series.

See RFC 1757 for more information about the RMON MIB.

Examples

The following example enables the **rmon event** command:

```
rmon event 1 log trap eventtrap description "High ifOutErrors" owner sdurham
```

This example configuration creates RMON event number 1, which is defined as High ifOutErrors, and generates a log entry when the event is triggered by an alarm. The user sdurham owns the row that is created in the event table by this command. This configuration also generates a Simple Network Management Protocol (SNMP) trap when the event is triggered.

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
show rmon	Displays the current RMON agent status on the router.

rmon queuesize

To change the size of the queue that holds packets for analysis by the Remote Monitoring (RMON) process, use the **rmon queuesize** command in global configuration mode. To restore the default value, use the **no** form of this command.

rmon queuesize *size*

no rmon queuesize

Syntax Description

size	Number of packets allowed in the queue awaiting RMON analysis. Default queue size is 64 packets.

Defaults

64 packets

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command applies to the RMON function, which is available on Ethernet interfaces of Cisco 2500 series and Cisco AS5200 series routers only.

You might want to increase the queue size if the RMON function indicates it is dropping packets. You can determine this from the output of the **show rmon** command or from the etherStatsDropEvents object in the etherStats table. A feasible maximum queue size depends on the amount of memory available in the router and the configuration of the buffer pool.

Examples

The following example configures the RMON queue size to be 128 packets:

```
Router(config)# rmon queuesize 128
```

Related Commands

Command	Description
show rmon	Displays the current RMON agent status on the router.

rommon-pref

To select a ReadOnly or Upgrade ROMmon image to be booted on the next reload of a Cisco 7200 VXR router or Cisco 7301 router when you are in ROMmon, use the **rommon-pref** command in ROMmon mode.

rommon-pref [**readonly** | **upgrade**]

Syntax Description

readonly	Selects the ReadOnly ROMmon image to be booted on the next reload.
upgrade	Selects the Upgrade, second ROMmon image to be booted on the next reload.

Defaults

No default behavior or values

Command Modes

ROMmon

Command History

Release	Modification
12.0(28)S	This command was introduced on the Cisco 7200 VXR router. It was introduced in ROMmon version 12.3(4r)T1 for the Cisco 7200 VXR router.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T and supported on the Cisco 7200 VXR router and Cisco 7301 router. It was introduced in ROMmon version 12.3(4r)T2 for the Cisco 7301 router.
12.3(9)	This command was integrated into Cisco IOS Release 12.3(9) and supported on the Cisco 7200 VXR router and Cisco 7301 router.

Usage Guidelines

You might select the ReadOnly ROMmon image to be booted on the next reload because the Upgrade image has features or side effects you do not like.

When you are in ROMmon, there is no descriptive output to inform you whether the ReadOnly ROMmon image was reloaded. To confirm the reload, use the **showmon** command after entering the **rommon-pref readonly** command.

Use this command when you are in ROMmon mode. Use the **upgrade rom-monitor preference** command when you are in Cisco IOS.

Examples

The following example, applicable to both the Cisco 7200 VXR and Cisco 7301 routers, shows how to select the ReadOnly ROMmon image to be booted on the next reload of the router when you are already in ROMmon mode:

```
rommon 2 > rommon-pref readonly
```

Related Commands

Command	Description
showmon	Shows both the ReadOnly and the Upgrade ROMmon image versions when you are in ROMmon mode, as well as which ROMmon image is running.

rsh

To execute a command remotely on a remote shell protocol (rsh) host, use the **rsh** command in privileged EXEC mode.

rsh {*ip-address* | *host*} [**/user** *username*] *remote-command*

Syntax Description

ip-address	IP address of the remote host on which to execute the **rsh** command. Either the IP address or the host name is required.
host	Name of the remote host on which to execute the command. Either the host name or the IP address is required.
/user *username*	(Optional) Remote username.
remote-command	Command to be executed remotely.

Defaults

If you do not specify the **/user** *username* keyword and argument, the Cisco IOS software sends a default remote username. As the default value of the remote username, the software sends the username associated with the current tty process, if that name is valid. For example, if the user is connected to the router through Telnet and the user was authenticated through the **username** command, then the software sends that username as the remote username. If the tty username is invalid, the software uses the host name as the both the remote and local usernames.

Note For Cisco, tty lines are commonly used for access services. The concept of tty originated with UNIX. For UNIX systems, each physical device is represented in the file system. Terminals are sometimes called tty devices (tty stands for teletype, the original UNIX terminal).

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use the **rsh** command to execute commands remotely. The host on which you remotely execute the command must support the rsh protocol, and the *.rhosts* files on the rsh host must include an entry that permits you to remotely execute commands on that host.

For security reasons, the software does not default to a remote login if no command is specified, as does UNIX. Instead, the router provides Telnet and connect services that you can use rather than rsh.

Examples

The following command specifies that the user named sharon attempts to remotely execute the UNIX **ls** command with the *-a* argument on the remote host named mysys.cisco.com. The command output resulting from the remote execution follows the command example:

```
Router1# rsh mysys.cisco.com /user sharon ls -a
.
.
.
.alias
.cshrc
.emacs
.exrc
.history
.login
.mailrc
.newsrc
.oldnewsrc
.rhosts
.twmrc
.xsession
jazz
```

rtr key-chain

To enable Service Assurance Agent (SAA) control message authentication and specify an MD5 key chain, use the **rtr key-chain** command in global configuration mode. To remove control message authentication, use the **no** form of this command.

rtr key-chain *name*

no rtr key-chain

Syntax Description

name	Name of MD5 key chain.

Defaults

Control message authentication is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

The authentication configuration on the SAA collector and SAA Responder must be the same. Both sides must configure the same key chain or both sides must not use authentication.

Examples

In the following example, the SAA control message uses MD5 authentication, and the key chain name is CSAA:

```
Router(config)# rtr key-chain csaa
```

Related Commands

Command	Description
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.

rtr low-memory

To specify how much unused memory must be available to allow Service Assurance Agent (SAA) configuration, use the **rtr low-memory** command in global configuration mode. To remove the type configuration for the operation, use the **no** form of this command.

rtr low-memory *value*

no rtr low-memory

Syntax Description

value	Specifies amount of memory, in bytes, that must be available to configure SAA (RTR). The range is from 0 to the maximum amount of free memory bytes available.

Defaults

The default *value* is 25 percent of the memory available on the system.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

The **rtr low-memory** command allows the user to specify the amount of memory that the SAA can use. If the amount of available free memory falls below the value specified in the **rtr low-memory** command, then the SAA will not allow new operations to be configured. If this command is not used, the default low-memory value is 25 percent. This means that if 75 percent of system memory has been utilized you will not be able to configure any SAA characteristics.

The value of the **rtr low-memory** command should not exceed the amount of free memory available on the system. To determine the amount of free memory available on the system, use the **show memory** EXEC command.

Examples

In the following example, the router is configured so that no less than 2 MB of memory will be free for RTR configuration:

```
Router(config)# rtr low-memory 2000000
```

Related Commands

Command	Description
rtr	Specifies an identification number for an operation and enters SAA RTR configuration mode.
show memory	Displays statistics about memory, including memory-free pool statistics.

rtr reaction-configuration

To configure certain actions to occur based on events under the control of the Service Assurance Agent (SAA), use the **rtr reaction-configuration** command in global configuration mode. To return to the default values of the operation, use the **no** form of this command.

rtr reaction-configuration *operation-number* [**verify-error-enable**] [**connection-loss-enable**] [**timeout-enable**] [**threshold-falling** *milliseconds*] [**threshold-type** *option*] [**action-type** *option*]

no rtr reaction-configuration *operation-number*

Syntax Description

operation-number	Number of the SAA operation to configure.
verify-error-enable	(Optional) Enables error verification. The default is disabled.
connection-loss-enable	(Optional) Enables checking for connection loss in connection-oriented protocols. Disabled by default.
timeout-enable	(Optional) Enables checking for response time reporting operation timeouts based on the timeout value configured for the operation with the **timeout** SAA RTR configuration command. The default is disabled.
threshold-falling *milliseconds*	(Optional) Sets the falling threshold (standard RMON-type hysteresis mechanism) in milliseconds. When the falling threshold is met, generate a resolution reaction event. The rising of the operation over threshold is set with the **threshold** SAA RTR configuration command. The default value is 3000 ms.
threshold-type *option*	(Optional) Specify the algorithm used by the SAA to calculate over and falling threshold violations. The value for *option* can be one of the following keywords: • **never**—Do not calculate threshold violations (the default). • **immediate**—When the response time exceeds the rising over threshold or drops below the falling threshold, immediately perform the action defined by **action-type**. • **consecutive** [*occurrences*]—When the response time exceeds the rising threshold consecutively five times or drops below the falling threshold consecutively five times, perform the action defined by **action-type**. Optionally specify the number of consecutive occurrences. The default is 5. • **xofy** [*x-value y-value*]—When the response time exceeds the rising threshold five out of the last five times or drops below the falling threshold five out of the last five times, perform the action defined by **action-type**. Optionally specify the number of violations that must occur and the number that must occur within a specified number. The default is 5 for both x-value and y-value.

	• **average** [*attempts*]—When the average of the last five response times exceeds the rising threshold or when the average of the last five response times drops below the falling threshold, perform the action defined by **action-type**. Optionally specify the number of operations to average. The default is the average of the last five response time operations. For example: if the threshold of the operation is 5000 ms and the last three attempts results of the operation are 6000, 6000, and 5000 ms, the average would be 6000 + 6000 + 5000=17000/3 > 5000, thus violating the 5000-ms threshold.
action-type *option*	(Optional) Specify what action or combination of actions the operation performs when you configure **connection-loss-enable** or **timeout-enable**, or threshold events occur. For the **action-type** to occur for threshold events, the **threshold-type** must be defined to anything other than **never**. Option can be one of the following keywords: • **none**—No action is taken. • **trapOnly**—Send an SNMP trap on both over and falling threshold violations. • **nmvtOnly**—Send an SNA NMVT Alert on over threshold violation and an SNA NMVT Resolution on falling threshold violations. • **triggerOnly**—Have one or more target operation's operational state make the transition from "pending" to "active" on over (and falling) threshold violations. The target operations are defined with the **rtr reaction-trigger** command. A target operation will continue until its life expires as specified by the target operation's life value configured with the **rtr schedule** global configuration command. A triggered target operation must finish its life before it can be triggered again. • **trapAndNmvt**—Send a combination of **trapOnly** and **nmvtOnly**. • **trapAndTrigger**—Send a combination of **trapOnly** and **triggerOnly**. • **nmvtAndTrigger**—Send a combination of **nmvtOnly** and **triggerOnly**. • **trapNmvtAndTrigger**—Send a combination of **trapOnly**, **nmvtOnly**, and **triggerOnly**.

Defaults

No reactions are generated.

Error verification is disabled.

Connection loss is disabled.

Checking the timeout is disabled.

The falling threshold value is 3000 ms.

The algorithm threshold is **never**.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.1(1)T	The **verify-error-enable** optional keyword was added.

Usage Guidelines

Triggers are used for diagnostics purposes and are not used in normal operation.

You can use triggers to assist you in determining where delays are happening in the network when excessive delays are being seen on an end-to-end basis.

The reaction applies only to attempts to the target (that is, attempts to any hops along the path in **pathEcho** do not generate reactions).

Note Keywords are not case sensitive and are shown in mixed case for readability only.

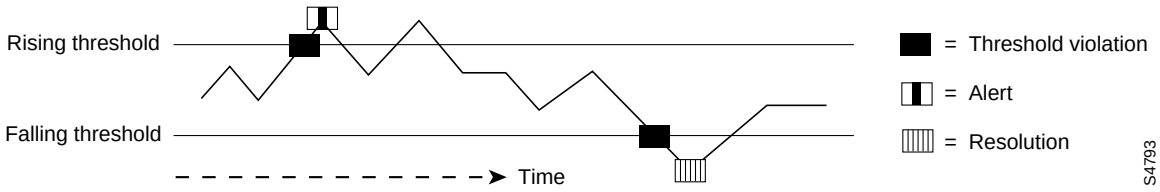
Examples

In the following example, operation 19 sends an SNMP trap when there is an over or falling threshold violation:

```
Router(config)# rtr reaction-configuration 19 threshold-type immediate action-type
trapOnly
```

Figure 1 shows that an alert (rising trap) would be issued immediately when the response time exceeds the rising threshold and a resolution (falling trap) would be issued immediately when the response time drops below the falling threshold.

Figure 1 Example of Rising and Falling Thresholds



Related Commands

Command	Description
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.
rtr reaction-trigger	Defines a second SAA operation to make the transition from a pending state to an active state when one of the trigger action-type options are defined with the **rtr reaction-configuration** global configuration command.
threshold	Sets the rising threshold (hysteresis) that generates a reaction event and stores history information for the SAA operation.
timeout	Sets the amount of time the SAA operation waits for a response from its request packet.

rtr reaction-trigger

To define a second Service Assurance Agent (SAA) operation to make the transition from a pending state to an active state when one of the trigger action-type options are defined with the **rtr reaction-configuration** command, use the **rtr reaction-trigger** command in global configuration mode. To remove the trigger combination, use the **no** form of this command.

rtr reaction-trigger *operation-number target-operation*

no rtr reaction-trigger *operation*

Syntax Description

operation-number	Number of the operation in the active state that has the **action-type** set with the **rtr reaction-configuration** global configuration command.
target-operation	Number of the operation in the pending state that is waiting to be triggered with the **rtr** global configuration command.

Defaults

No trigger combination is defined.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Triggers are usually used for diagnostics purposes and are not used in normal operation.

Examples

In the following example, the state of operation 1 is changed from pending state to active state when **action-type of** operation 2 occurs:

```
Router(config)# rtr reaction-trigger 2 1
```

Related Commands

Command	Description
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.
rtr reaction-configuration	Configures certain actions to occur based on events under the control of the SAA.
rtr schedule	Configures the time parameters for an SAA operation.

rtr reset

To perform a shutdown and restart of the Service Assurance Agent engine, use the **rtr reset** command in global configuration mode.

rtr reset

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The **rtr reset** command stops all operations, clears SAA/RTR configuration information, and returns the SAA feature to the startup condition. This command does not reread the SAA RTR configuration stored in startup-config in NVRAM. You must retype the configuration or load a previously saved configuration file.

Caution Use the **rtr reset** command only in extreme situations such as the incorrect configuration of a number of operations.

Examples

The following example resets SAA, clearing all stored SAA information and configuration:

```
Router(config)# rtr reset
```

Related Commands

Command	Description
rtr restart	Restarts a stopped SAA operation.

rtr responder

To enable the Service Assurance Agent (SAA) Responder for general SAA operations, use the **rtr responder** command in global configuration mode. To disable the SAA Responder, use the **no** form of this command.

rtr responder

no rtr responder

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

This command is used on the destination device for SAA operations to enable the sending of receiving of RTR Control packets. Enabling the SAA/RTR Responder allows the generation of packet loss statistics on the device sending SAA operations.

Examples

The following example enables the SAA Responder:

```
Router(config)# rtr responder
```

Related Commands

Command	Description
rtr responder type tcpConnect	Enables the SAA Responder for TCP Connect operations.
rtr responder type udpEcho	Enables the SAA Responder for UDP Echo and Jitter operations.

rtr responder type frame-relay

To enable the Service Assurance Agent (SAA) Responder on the operational target device for Frame Relay operations, use the **rtr responder type frame-relay** command in global configuration mode. To disable the SAA Responder, use the **no** form of this command.

rtr responder type frame-relay {**all** | **interface** {**serial** | **fr-atm**} *interface-id* **dlci** *dlci-number*}

no rtr responder type frame-relay {**all** | **interface** {**serial** | **fr-atm**} *interface-id* **dlci** *dlci-number*}

Syntax Description

all	Specifies that the SAA Responder will respond to Frame Relay operations on every interface and DLCI.
interface serial	Specifies the serial interface over which to respond to Frame Relay operations.
interface fr-atm	Specifies the Frame Relay interface over which to respond to Frame Relay operations.
interface-number	Frame Relay or Serial interface number.
dlci *dlci-number*	Specifies the Frame Relay PVC subinterface link (DLCI number) that is assigned to the interface.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

This command allows the SAA Responder to respond to Frame Relay operations without receiving RTR Control Protocol packets.

Note that if you use this command, packet loss statistics will not be able to be generated for the operation because the Responder will not be able to determine the order of the received packets. To generate packet loss statistics, use the **rtr responder** command without specifying an operation type.

Examples

In the following example, the SAA Responder is configured to respond to Frame Relay operations specifically on Serial interface 1/0, using DLCI number 16:

```
Router(config)# rtr responder type frame-relay interface serial1/0 dlci 16
```

Related Commands

Command	Description
rtr	Specifies an SAA operation and enters RTR Entry configuration mode.

rtr responder type tcpConnect

To enable the Service Assurance Agent (SAA) Responder for TCP Connect operations, use the **rtr responder type tcpConnect** command in global configuration mode. To disable the SAA Responder, use the **no** form of this command.

rtr responder type tcpConnect ipaddress *ip-address* **port** *port*

no rtr responder type tcpConnect ipaddress *ip-address* **port** *port*

Syntax Description

ipaddress *ip-address*	(Optional) Specifies the IP address that the operation will be received at.
port *port*	(Optional) Specifies the port number that the operation will be received on.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.1(1)T	The **ipaddr** and **port** keywords were added.

Usage Guidelines

This command is used on the destination device for SAA operations to enable the acceptance and return of TCP Connect operation packets.

Related Commands

Command	Description
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.
rtr responder type frame-relay	Enables the SAA Responder for Frame Relay operations.
rtr responder type udpEcho	Enables the SAA Responder for UDP Echo and Jitter operations.

rtr responder type udpEcho

To enable the Service Assurance Agent (SAA) Responder for User Datagram Protocol (UDP) Echo or Jitter operations, use the **rtr responder** command in global configuration mode. To disable the SAA Responder, use the **no** form of this command.

rtr responder type udpEcho ipaddress *ip-address* **port** *port*

no rtr responder type udpEcho ipaddress *ip-address* **port** *port*

Syntax Description

ipaddress *ip-address*	Specifies the IP address that the operation will be received at.
port *port*	Specifies the port number that the operation will be received on.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

This command is used on the destination device for SAA operations to enable UPD Echo and Jitter (UDP+) operations on non-native interfaces.

Examples

The following example enables the SAA Responder for Jitter operations:

```
Router(config)# rtr responder type udpEcho ipaddress A.B.C.D port 1
```

Related Commands

Command	Description
rtr responder	Enables the SAA Responder for non-specific SAA operations.
rtr responder type frame-relay	Enables the SAA Responder for Frame Relay operations.

rtr restart

To restart an Service Assurance Agent (SAA) operation, use the **rtr restart** command in global configuration mode.

rtr restart *operation-number*

Syntax Description

operation-number	Number of the SAA operation to restart. SAA allows a maximum of 2000 operations.

Defaults

No default behavior or values.

Command Modes

Global configuration.

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	The maximum number of operations was increased from 500 to 2000 (SAA Engine II).

Usage Guidelines

To restart an operation, the operation should be in an "active" state (as defined in the **rtr reaction-configuration** command).

SAA allows a maximum of 2000 operations.

This command does not have a no form.

Examples

The following example restarts operation 12:

```
Router(config)# rtr restart 12
```

Related Commands

Command	Description
rtr reset	Clears all current SAA/RTR statistics and configuration information from the router and resets the SAA engine.

rtr schedule

To configure the time parameters for an Service Assurance Agent (SAA) operation, use the **rtr schedule** command in global configuration mode. To stop the operation and place it in the default state (**pending**), use the **no** form of this command.

rtr schedule *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm*[:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*::*ss*}] [**ageout** *seconds*]

no rtr schedule *operation-number*

Syntax Description

operation-number	Number of the SAA operation to schedule.
life *seconds*	(Optional) Number of seconds the operation actively collects information. The default is 3600 seconds (one hour).
life forever	(Optional) Schedules the operation to run indefinitely.
start-time	(Optional) Time when the operation starts collecting information. If the **start-time** is not specified, no information is collected until the **start-time** is configured or a trigger occurs that performs a **start-time now**.
start-time *hh***:***mm*[**:***ss*]	(Optional) Specifies an absolute start time using hour, minute, and (optionally) second. Use the 24-hour clock notation. For example, **start-time 01:02** means "start at 1:02 a.m.," and **start-time 13:01:30** means "start at 1:01 p.m. and 30 seconds." The current day is implied unless you specify a *month* and *day*.
month	(Optional) Name of the month to start the operation in. If month is not specified, the current month is used. Use of this argument requires that a day be specified as well. You can specify the month with the full english name, or using the first three letters of the month.
day	(Optional) Number of the day (in the range 1 to 31) to start the operation on. If a day is not specified, the current day is used. Use of this argument requires that a month be specified as well.
start-time pending	(Optional) No information is collected. This is the default value.
start-time now	(Optional) Indicates that the operation should start immediately.
start-time after *hh***:***mm***:***ss*	(Optional) Indicates that the operation should start *hh* hours, *mm* minutes, and *ss* seconds after this command was entered.
ageout *seconds*	(Optional) Number of seconds to keep the operation in memory when it is not actively collecting information. The default is 0 seconds (never ages out).

Defaults

The operation is placed in a **pending** state (that is, the operation is enabled but not actively collecting information).

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.1(1)T	The **after** and **forever** keywords were added.

Usage Guidelines

After you schedule the operation with the **rtr schedule** command, you cannot change the configuration of the operation. To change the configuration of the operation, use the **no** form of the **rtr** global configuration command and reenter the configuration information.

If the operation is in a pending state, you can define the conditions under which the operation makes the transition from pending to active with the **rtr reaction-trigger** and **rtr reaction-configuration** global configuration commands. When the operation is in an active state, it immediately begins collecting information.

The following time line shows the age-out process of the operation:

```
W----------------------X----------------------Y----------------------Z
```

where:

- W is the time the operation was configured with the **rtr** global configuration command.
- X is the start time or start of life of the operation (that is, when the operation became “active”).
- Y is the end of life as configured with the **rtr schedule** global configuration command (life seconds have counted down to zero).
- Z is the age out of the operation.

Age out starts counting down at W and Y, is suspended between X and Y, and is reset to its configured size at Y.

It is possible for the operation to age out before it executes (that is, Z can occur before X). To ensure that this does not happen, the difference between the operation’s configuration time and start time (X and W) must be less than the age-out seconds.

Note The total RAM required to hold the history and statistics tables is allocated at this time. This is to prevent router memory problems when the router gets heavily loaded and to lower the amount of overhead the feature causes on a router when it is active.

For SLM operations (**type slm**), the operation will always start at the nearest 15 minute interval since the router start time. For example, if the **rtr schedule 1 start-time now** command is used, the operation will not start until the next quarter-hour time increment.

Examples

In the following example, operation 25 begins actively collecting data at 3:00 p.m. on April 5. This operation will age out after 12 hours of inactivity, which can be before it starts or after it has finished with its life. When this operation ages out, all configuration information for the operation is removed (that is, the configuration information is no longer in the running-config in RAM).

```
Router(config)# rtr schedule 25 life 43200 start-time 15:00 apr 5 ageout 43200
```

In the following example, operation 1 begins collecting data after a 5 minute delay:

```
Router(config)# rtr schedule 1 start after 00:05:00
```

In the following example, operation 3 begins collecting data immediately and is scheduled to run indefinitely:

```
Router(config)# rtr schedule 3 start-time now life forever
```

Related Commands

Command	Description
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.
rtr reaction-configuration	Configures certain actions to occur based on events under the control of the SAA.
rtr reaction-trigger	Defines a second SAA operation to make the transition from a pending state to an active state when one of the trigger action-type options is defined with the **rtr reaction-configuration** global configuration command.

rtr

To begin configuring an Service Assurance Agent (SAA) operation by entering SAA RTR configuration mode, use the **rtr** command in global configuration mode. To remove all configuration information for an operation, including the schedule of the operation, reaction configuration, and reaction triggers, use the **no** form of this command.

rtr *operation-number*

no rtr *operation-number*

Syntax Description

operation-number	Operation number used for the identification of the SAA operation you wish to configure.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(11)T	The maximum number of operations was increased from 500 to 2000 (SAA Engine II).

Usage Guidelines

The **rtr** command is used to configure Cisco Service Assurance Agent (SAA) operations. Use this command to specify an identification number for the operation you are about to configure. After you enter this command, you will enter the SAA RTR configuration mode, indicated by the `(config-rtr)` router prompt. The "Related Commands" table lists the commands you can use in SAA RTR configuration mode.

For detailed information on the configuration of the Cisco SAA feature, see the "Network Monitoring Using Cisco Service Assurance Agent" chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

SAA allows a maximum of 2000 operations.

Debugging is supported only on the first 32 operation numbers.

After you configure a operation, you must schedule the operation. For information on scheduling a operation, refer to the **rtr schedule** global configuration command. You can also optionally set reaction triggers for the operation. For information on reaction triggers, refer to the **rtr reaction-configuration** and **rtr reaction-trigger** global configuration commands.

Note After you schedule an operation with the **rtr schedule** global configuration command, you cannot modify the configuration of the operation. To modify the configuration of the operation after it is scheduled, use the **no rtr** command. You can now reenter the operation's configuration with the **rtr** command.

To display the current configuration settings of the operation, use the **show rtr configuration** EXEC command.

Examples

In the following example, operation 1 is configured to perform end-to-end response time operations using an SNA LU Type 0 connection with the host name cwbc0a. Only the **type** SAA RTR configuration command is required; all others are optional.

```
Router(config)# rtr 1
Router(config-rtr)# type echo protocol snalu0echoappl cwbc0a
Router(config-rtr)# request-data-size 40
Router(config-rtr)# response-data-size 1440
Router(config-rtr)# exit
Router(config)#
```

Note If operation 1 already existed and it has not been scheduled, you are placed into SAA RTR configuration command mode. If the operation already exists and has been scheduled, this command will fail.

Related Commands

Command	Description
buckets-of-history-kept	Sets the number of history buckets that are kept during an SAA operation's lifetime.
distributions-of-statistics-kept	Sets the number of statistic distributions kept per hop during an SAA operation's lifetime.
filter-for-history	Defines the types of information to be kept in the history table for SAA operations.
frequency	Sets the frequency at which the operation should execute.
hops-of-statistics-kept	Sets the number of hops for which statistics are maintained per path for the SAA operation.
hours-of-statistics-kept	Sets the number of hours for which statistics are maintained for SAA operations.
lives-of-history-kept	Sets the number of lives maintained in the history table for an SAA operation.
lsr path	Specifies the path on which to measure the ICMP Echo response time.
owner	Configures the SNMP owner of an SAA operation.
paths-of-statistics-kept	Sets the number of paths for which statistics are maintained per hour for an SAA operation.
request-data-size	Sets the protocol data size in the payload of an operation's request packet.
response-data-size	Sets the protocol data size in the payload of an operation's response packet.

Command	Description
samples-of-history-kept	Sets the number of entries kept in the history table for an SAA operation.
statistics-distribution-interval	Sets the time interval for each statistical distribution.
tag	Logically links SAA operations together in a group.
threshold	Sets the rising threshold (hysteresis) that generates a reaction event and stores history information for the probe.
timeout	Sets the amount of time an SAA operation waits for a response from its request packet.
tos	Defines the IP type of service for request packets of SAA operations.
type dlsw	Configures an SAA DLSw operation.
type tcpConnect	Defines an SAA TCP Connect operation.
verify-data	Checks each SAA operation response for corruption.

rtr slm frame-relay statistics

To enable the Service Assurance Agent (SAA) or Cisco Networking Services (CNS) to collect Frame Relay performance monitoring statistics, use the **rtr slm frame-relay statistics** command in global configuration mode. To disable the collection of Frame Relay performance monitoring statistics, use the **no** form of this command.

rtr slm frame-relay statistics

no rtr slm frame-relay statistics

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

The **rtr slm frame-relay statistics** command should be issued prior to configuring any of the Frame Relay service level monitoring SAA operations (**type slm interface**, **type slm controller**, **type slm frame-relay** or **type slm frame-relay pvc**). Performance statistics are not retained for these operations until this command is issued.

This command does not affect the standard Frame Relay SAA operation (**type frame-relay**).

Examples

In the following example the SAA Frame Relay service level monitoring feature is enabled:

```
Router(config)# rtr slm frame-relay statistics
```

Related Commands

Command	Description
type slm controller	Specifies that the SAA operation is an SLM controller operation, and specifies the controller that the operation should be run on.
type slm frame-relay interface	Specifies that the SAA operation is an SLM FR interface operation, and specifies the interface that the operation should be run on.
type slm frame-relay pvc interface	Specifies that the SAA operation is an SLM FR circuit operation, and specifies the interface and DLCI number that the operation should be run on.
type slm interface	Specifies that the SAA operation is an SLM interface operation, and specifies the interface that the operation should be run on.

saa apm cache-size

To set the size of the Service Assurance Agent (SAA) Application Performance Monitor (APM) cache, use the **saa apm cache-size** command in global configuration mode. To reset the SAA APM cache size to its default, use the **no** form of this command.

saa apm cache-size *bytes*

no saa apm cache-size *bytes*

Syntax Description

bytes	Number that specifies the size of the cache, in bytes. The default is 100000 bytes.

Defaults

The default APM cache size is 100000 bytes.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

SAA APM script and scheduler files are kept in an area of memory called the SAA APM cache. The cache size is checked by the system before each attempt to copy a new file to the cache. If the file to be downloaded puts the cache over its size limit, a "cache trimming" operation is performed, and all files in the cache not tagged with a "sticky bit" (sticky=1) will be deleted.

Examples

In the following example, the SAA APM cache is set to 80,000 bytes (approximately 78 kilobytes):

```
Router(config)# saa apm cache-size 80000
Router(config)# end
Router#
00:01:50: %SYS-5-CONFIG_I: Configured from console by console
Router# show saa apm cache

 Cache Size (bytes): 80000
 Cache used (bytes): 793

 File Name                                TimeCreated TimeAccessed ref Type sticky
 apm.cf.1234567                              00:02:50     00:00:00   1 CFG  0
 apm/config/smtp-1000.cfg                    00:02:50     00:00:00   1 CFG  0
```

Related Commands

Command	Description
show saa apm cache	Displays the amount of memory available in the SAA APM cache and information about the files stored in the cache.

saa apm copy

To copy script or scheduler files from an FTP server to the device that will initiate the Service Assurance Agent (SAA) Application Performance Monitor (APM) operations, use the **saa apm copy** command in global configuration mode.

saa apm copy {**script** | **scheduler**} **ftp:**//[*username***:***password***@**]*server-name/path-to-file/filename* [**sticky**]

Syntax Description

script	Specifies that the file to be copied is an APM script file (.scr).
scheduler	Specifies that the file to be copied is an APM scheduler file (.sch).
ftp://	Begins the URL that specifies the file to copy from a remote FTP server.
*username***:***password***@**	(Optional) Specifies a username and password as part of the URL. Use these arguments only if they are required on the server.
server-name	The server-name component of the URL.
path-to-file	Folder-path component of the URL. A folder-path can contain multiple folder names. Each folder should be separated using a forward slash (/).
filename	Name of the file to be copied from the server.
sticky	(Optional) Indicates that the copied file should not be deleted from the local APM cache during a cache trimming operation.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

The **saa apm copy** command downloads an SAA APM script or scheduler file from an FTP server to the local SAA APM cache in NVRAM.

A file tagged as “sticky” will not be deleted from the local APM cache during a cache trimming operation. APM cache trimming operations are initiated when the **saa apm lowWaterMark** value is reached.

You can force a file tagged as “sticky” to be deleted using the **clear saa apm cache** command.

Examples

In the following example, a Frame Relay emulation script titled frm.scr is downloaded from the FTP server FTP101. The username joe and the password letmein are used to access the server:

```
Router(config)# saa apm copy script ftp://joe:letmein@FTP101/userbin/joefiles/frm.scr
sticky
```

Related Commands

Command	Description
clear saa apm cache	Deletes files from the SAA APM cache.
saa apm lowWaterMark	Specifies the lowest amount of free memory that must be available on the system to allow additional SAA APM operations to be configured.

saa apm lowWaterMark

To specify the lowest amount of free memory that must be available on the system to allow additional Service Assurance Agent (SAA) Application Performance Monitor (APM) operations to be configured, use the **saa apm lowWaterMark** command in global configuration mode. To restore the default low-memory-watermark value, use the **no** form of this command.

saa apm lowWaterMark *bytes*

no saa apm lowWaterMark

Syntax Description

bytes	Number that specifies the size of the cache, in bytes.

Defaults

The default APM low-memory-watermark is 25 percent of free memory at startup.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

The **saa apm lowWaterMark** global configuration command configures the lowest amount of free memory (low-memory-watermark) that must be available on the system. If the amount of available free memory falls below the value specified in the **saa apm lowWaterMark** command, then the SAA will not allow new APM operations to be configured. The default value is 25 percent of the memory available on the system at startup.

Note The smaller the low-memory-watermark value is, the more APM operations can be configured. If the value is set to 0, then APM operations can be created until the system runs out of memory. However, you should be careful not to set the low-memory-watermark too low, as all additional router processes must be able to run with the amount of memory specified by the **saa apm lowWaterMark** and **rtr low-memory** commands. Setting the low-memory-watermark to 0 is discouraged, as other router processes may not be left with enough system memory to function.

For example, if there are 6 MB of free memory when the router starts up, and the default low-memory-watermark of 25 percent is used, then the SAA APM can use up to 4.5 MB memory for creating operations. If the free memory drops below 1.5 MB, then new APM operations cannot be created.

The value of the **saa apm lowWaterMark** command should not exceed the amount of free memory available on the system. To determine the amount of free memory available on the system, use the **show memory** EXEC command.

The **show saa apm information** EXEC command will display the number of operations that can be configured on the device in the "Max Number of operations supported" field.

Examples

In the following example, the SAA APM low-memory-watermark is set to 3,145,728 bytes (3 MB):

```
Router(config)# saa apm lowWaterMark 3145728
Router(config)# end
Router# show saa apm information
        Service Assurance Agent: Application Performance Monitor

          APM Engine Version: 1.0
Max Number of oper supported: 23
 Number of configurable oper: 23
   Number of oper configured: 0
    Number of files in cache: 0
          Cache Size (bytes): 100000
          Cache used (bytes): 0
   APM low memory water-mark: 3,145,728
```

Related Commands

Command	Description
show saa apm information	Displays details about the SAA APM.

saa apm operation

To start or stop an Service Assurance Agent (SAA) Application Performance Monitor (APM) operation, use the **saa apm operation** command in global configuration mode. To delete existing SAA APM operations, use the **no** form of this command.

saa apm operation *operation-number* {**start**
ftp://[*user***:***password***@**]*server-name*/*path-to-file*/*filename* | **stop**}

no saa apm operation [*operation-number*]

Syntax Description

operation-number	A number which uniquely identifies the APM operation. In the **no saa apm operation** form of this command, this argument is optional. If an operation-number is not specified in the **no** form of this command, all APM operations are removed from the system configuration.
start	Starts the specified operation.
ftp://	Begins the URL that specifies the configuration file to use for the APM operation.
*user***:***password***@**	(Optional) Allows you to specify a user-name and password as part of the URL if they are required on the server.
server-name	Server-name component of the URL.
path-to-file	Folder path component of the URL. Each folder should be separated using a forward slash (/).
filename	Name of the APM configuration (.cf) file to be used for the operation.
stop	Stops the specified operation.

Defaults

No SAA APM operations exist.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

The following files are required to perform an SAA APM operation:

- script file (.scr) available on the routing device running SAA
- scheduler file (.sch) available on the routing device running SAA
- configuration file (.cf) available on an FTP server
- data file (.dat) available on an FTP server

All filenames can have a maximum of 255 characters.

The **saa apm operation start** command points to the APM configuration file to be used for the operation. The APM configuration file specifies the location of the other files used in the operation, and the target IP address for the operation.

To download script, configuration, data, and scheduler template files used by the SAA APM, and to download the documentation ("readme" files) for the scripts, go to the "Cisco SAA APM" page at http://www.cisco.com/cgi-bin/tablebuild.pl/saa-apm.

After an operation is started using the **saa apm operation start** command, the operation should be stopped using the **saa apm operation stop** command.

Examples

In the following example, an SAA APM NNTP operation is started and stopped, and the operation is deleted from the configuration:

```
Router# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# saa apm operation 2 start
ftp://user:password@saa-nms/apm/config/nntp-20.cf
Router(config)#
1d09h: SAA-APM-1: downloading file (apm/config/nntp-20.cf) of size (532)
1d09h: SAA-APM-1: using cached file (apm/scheduler/master.sch)
1d09h: SAA-APM-1: using cached file (apm/scripts/nntp.scr)
1d09h: SAA-APM-1: sending APM_SCRIPT_DONE message
1d09h: SAA-APM-1: operation done
Router(config)# saa apm operation 2 stop
Router(config)# no saa apm operation 2
```

Related Commands

Command	Description
show saa apm results	Displays the data gathered using the SAA Application Performance Monitor.

samples-of-history-kept

To set the number of entries kept in the history table per bucket for the Service Assurance Agent (SAA) operation, use the **samples-of-history-kept** command in SAA RTR configuration mode. To return to the default value, use the **no** form of this command.

samples-of-history-kept *samples*

no samples-of-history-kept

Syntax Description

samples	Number of entries kept in the history table per bucket. The default is 16 entries for **type pathEcho** and 1 entry for **type echo**.

Defaults

16 entries for **type pathEcho**

1 entry for **type echo**

Command Modes

SAA RTR configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use the **samples-of-history-kept** command to control how many entries are saved in the history table. To control the type of information that gets saved in the history table, use the **filter-for-history** command. To set how many buckets get created in the history table, use the **buckets-of-history-kept** command.

An operation can collect history and capture statistics. By default, history is not collected. When a problem arises where history is useful (for example, a large number of timeouts are occurring), you can configure the **lives-of-history-kept** SAA RTR configuration command to collect history.

Note Collecting history increases the usage of RAM. Only collect history when you think there is a problem. For general network response time information, use statistics.

Examples

In the following example, ten entries are kept in the history table for each of the lives of operation 3:

```
Router(config)# rtr 1
Router(config-rtr)# type pathecho protocol ipIcmpEcho 172.16.1.176
Router(config-rtr)# lives-of-history-kept 3
Router(config-rtr)# samples-of-history-kept 10
```

Related Commands

Command	Description
buckets-of-history-kept	Sets the number of history buckets that are kept during the lifetime of the SAA.
filter-for-history	Defines the type of information kept in the history table for the SAA operation.
lives-of-history-kept	Sets the number of lives maintained in the history table for the SAA operation.
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.

scheduler allocate

To guarantee CPU time for processes, use the **scheduler allocate** command in global configuration mode. To restore the default, use the **no** form of this command.

scheduler allocate *interrupt-time process-time*

no scheduler allocate

Syntax Description

interrupt-time	Integer (in microseconds) that limits the maximum number of microseconds to spend on fast switching within any one network interrupt context. The range is from 400 to 60000 microseconds. The default is 4000 microseconds.
process-time	Integer (in microseconds) that guarantees the minimum number of microseconds to spend at the process level when network interrupts are disabled. The range is from 100 to 4000 microseconds. The default is 200 microseconds.

Defaults

Approximately 5 percent of the CPU is available for process tasks.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command applies to the Cisco 7200 series and Cisco 7500 series routers.

Note Changing settings associated with CPU processes can negatively impact system performance.

Examples

The following example makes 20 percent of the CPU available for process tasks:

```
Router(config)# scheduler allocate 2000 500
```

Related Commands

Command	Description
scheduler interval	Controls the maximum amount of time that can elapse without running system processes.

scheduler heapcheck process

To perform a "sanity check" for corruption in memory blocks when a process switch occurs, use the **scheduler heapcheck process** command in global configuration mode. To disable this feature, use the **no** form of this command.

scheduler heapcheck process [**memory** [**fast**] [**io**] [**multibus**] [**pci**] [**processor**] [**checktype** {**all** | **magic** | **pointer** | **refcount**}]]

no scheduler heapcheck process

Syntax Description

memory	(Optional) Specifies checking all memory blocks and memory pools.
fast	(Optional) Specifies checking the fast memory block.
io	(Optional) Specifies checking the I/O memory block.
multibus	(Optional) Specifies checking the multibus memory block.
pci	(Optional) Specifies checking the process control information (PCI) memory block.
processor	(Optional) Specifies checking the processor memory block.
checktype	(Optional) Specifies checking specific memory pools.
all	(Optional) Specifies checking the value of the block magic, red zone, size, refcount, and pointers (next and previous).
magic	(Optional) Specifies checking the value of the block magic, red zone, and size.
pointer	(Optional) Specifies checking the value of the next and previous pointers.
refcount	(Optional) Specifies checking the value of the block magic and refcount.

Defaults

This command is not enabled by default. If no keywords are specified, a sanity check will be performed on all the memory blocks and memory pools.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

When configuring this command, you can choose none or all memory block keywords (**fast**, **io**, **multibus**, **pci**, **processor**, and **checktype**).

Enabling this command has a significant impact on router performance.

Examples

The following example shows how to sanity check for corruption in the I/O memory block when a process switch occurs. In this example, the values of only the block magic, red zone, and size will be checked.

```
scheduler heapcheck process memory io checktype magic
```

The following example shows how to sanity check for corruption in the processor memory block when a process switch occurs. In this example, the values of only the next and previous pointers will be checked.

```
scheduler heapcheck process memory processor checktype pointer
```

Related Commands

Command	Description
memory sanity	Performs a “sanity check” for corruption in buffers and queues.

scheduler interval

To control the maximum amount of time that can elapse without running system processes, use the **scheduler interval** command in global configuration mode. To restore the default, use the **no** form of this command.

scheduler interval *milliseconds*

no scheduler interval

Syntax Description

milliseconds	Integer that specifies the interval (in milliseconds). The minimum interval that you can specify is 500 milliseconds; there is no maximum value.

Defaults

High-priority operations are allowed to use as much of the CPU as needed.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The normal operation of the network server allows the switching operations to use as much of the central processor as is required. If the network is running unusually heavy loads that do not allow the processor the time to handle the routing protocols, give priority to the system process scheduler. High-priority operations are allowed to use as much of the CPU as needed.

Note Changing settings associated with CPU processes can negatively impact system performance.

On the Cisco 7200 series and Cisco 7500 series, use the **scheduler allocate** global configuration command instead of the **scheduler interval** command.

Examples

The following example changes the low-priority process schedule to an interval of 750 milliseconds:

```
Router(config)# scheduler interval 750
```

Related Commands

Command	Description
scheduler allocate	Guarantees CPU time for processes.

send

To send messages to one or all terminal lines, use the **send** command in EXEC mode.

send {*line-number* | ***** | **aux** *number* | **console** *number* | **tty** *number* | **vty** *number*}

Syntax Description

line-number	Line number to which the message will be sent.
*****	Sends a message to all lines.
aux *number*	Sends a message to the specified AUX port.
console *number*	Sends a message to the specified console port.
tty *number*	Sends a message to the specified asynchronous line.
vty *number*	Sends a message to the specified virtual asynchronous line.

Defaults

No messages are sent.

Command Modes

User EXEC

Priviledged EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

After entering this command, the system prompts for the message to be sent, which can be up to 500 characters long. Enter **Ctrl-Z** to end the message. Enter **Ctrl-C** to abort this command.

Caution Be aware that in some circumstances text sent using the **send** command may be interpreted as an executable command by the receiving device. For example, if the receiving device is Unix workstation, and the receiving device is in a state (shell) where commands can be executed, the incoming text, if a properly formated Unix command, will be accepted by the workstation as a command. For this reason, you should limit your exposure to potential messages from terminal servers or other Cisco IOS-based devices when running an interactive shell.

Examples

The following example sends a message to all lines:

```
2509# send *
Enter message, end with CTRL/Z; abort with CTRL/C:
The system 2509 will be shut down in 10 minutes for repairs.^Z
Send message? [confirm]
2509#
***
***
*** Message from tty0 to all terminals:
***
```

```
The system 2509 will be shut down in 10 minutes for repairs.
```

server (boomerang)

To configure the server address for a specified boomerang domain, use the **server** command in boomerang configuration mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

server *server-ip-address*

no server *server-ip-address*

Syntax Description

server-ip-address	IP address of the specified server.

Defaults

No default behavior or values.

Command Modes

Boomerang configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

The **server** command can be used only on a Director Response Protocol (DRP) agent. The boomerang client is the Director Response Protocol (DRP) agent.

Use the **server** command to specify a server address that is to be associated with a given domain name. This configuration overrides the server-to-DRP agent association that is configured on DistributedDirector.

Examples

The following example configures the server for a domain named www.boom1.com. The server address for www.boom1.com is 172.16.101.101:

```
Router(config)# ip drp domain www.boom1.com
Router(config-boomerang)# server 172.16.101.101

Router# show running-config
.
.
.
ip drp domain www.boom1.com
content-server 172.16.101.101
```

Related Commands

Command	Description
alias (boomerang)	Configures an alias name for a specified domain.
ip drp domain	Adds a new domain to the DistributedDirector client or configures an existing domain and puts the client in boomerang configuration mode.

Command	Description
show ip drp	Displays DRP statistics on DistributedDirector or a DRP server agent.
show ip drp boomerang	Displays boomerang information on the DRP agent.
ttl dns	Configures the number of seconds for which an answer received from the boomerang client will be cached by the DNS client.
ttl ip	Configures the IP TTL value for the boomerang response packets sent from the boomerang client to the DNS client in number of hops.

service compress-config

To compress startup configuration files, use the **service compress-config** command in global configuration mode. To disable compression, use the **no** form of this command.

service compress-config

no service compress-config

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

After you configure the **service compress-config** command, the router will compress configuration files every time you save a configuration to the startup configuration. For example, when you enter the **copy system:running-config nvram:startup-config** command, the running configuration will be compressed before storage in NVRAM.

If the file compression succeeds, the following message is displayed:

```
Compressing configuration from configuration-size to compressed-size
[OK]
```

If the boot ROMs do not recognize a compressed configuration, the following message is displayed:

```
Boot ROMs do not support NVRAM compression Config NOT written to NVRAM
```

If the file compression fails, the following message is displayed:

```
Error trying to compress nvram
```

One way to determine whether a configuration file will be compressed enough to fit into NVRAM is to use a text editor to enter the configuration, then use the UNIX **compress** command to check the compressed size. To get a closer approximation of the compression ratio, use the UNIX **compress -b12** command.

Once the configuration file has been compressed, the router functions normally. At boot time, the system recognizes that the configuration file is compressed, uncompresses it, and proceeds normally. A **partition nvram:startup-config** command uncompresses the configuration before displaying it.

To disable compression of the configuration file, enter configuration mode and specify the **no service compress-config** command. Then, exit global configuration mode and enter the **copy system:running-config nvram:startup-config** command. The router displays an OK message if it is

able to write the uncompressed configuration to NVRAM. Otherwise, the router displays an error message indicating that the configuration is too large to store. If the configuration file is larger than the physical NVRAM, the following message is displayed:

```
##Configuration too large to fit uncompressed in NVRAM Truncate configuration? [confirm]
```

When the file is truncated, commands at the end of the file are erased. Therefore, you will lose part of your configuration. To truncate and save the configuration, type **Y**. To not truncate and not save the configuration, type **N**.

Examples

In the following example, the configuration file is compressed:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# service compress-config
Router(config)# end
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router# copy system:running-config nvram:startup-config
Building configuration...
Compressing configuration from 1179 bytes to 674 bytes
[OK]
```

Related Commands

Command	Description
partition nvram:startup-config	Separates Flash memory into partitions on Class B file system platforms.

service config

To enable autoloading of configuration files from a network server, use the **service config** command in global configuration mode. To restore the default, use the **no** form of this command.

service config

no service config

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled, except on systems without NVRAM or with invalid or incomplete information in NVRAM. In these cases, autoloading of configuration files from a network server is enabled automatically.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Usually, the **service config** command is used in conjunction with the **boot host** or **boot network** command. You must enter the **service config** command to enable the router to automatically configure the system from the file specified by the **boot host** or **boot network** command.

You no longer have to specify the **service config** command for the **boot host** or **boot network** command to be active.

If you specify both the **no service config** command and the **boot host** command, the router attempts to find the specified host configuration file. If you specify the **no service config** command, the **boot host** command is not active.

The **service config** command can also be used without the **boot host** or **boot network** command. If you do not specify host or network configuration filenames, the router uses the default configuration files. The default network configuration file is network-confg. The default host configuration file is host-confg, where host is the host name of the router. If the Cisco IOS software cannot resolve its host name, the default host configuration file is router-confg.

Examples

In the following example, a router is configured to autoload the default network and host configuration files. Because no **boot host** or **boot network** commands are specified, the router uses the broadcast address to request the files from a TFTP server.

```
Router(config)# service config
```

The following example changes the network configuration filename to bridge_9.1, specifies that rcp is to be used as the transport mechanism, and gives 172.16.1.111 as the IP address of the server on which the network configuration file resides:

```
Router(config)# service config
Router(config)# boot network rcp://172.16.1.111/bridge_9.1
```

Related Commands

Command	Description
boot host	Changes the default name of the host configuration filename from which to load configuration commands.
boot network	Changes the default name of the network configuration file from which to load configuration commands.

service decimal-tty

To specify that line numbers be displayed and interpreted as octal numbers rather than decimal numbers, use the **no service decimal-tty** command in global configuration mode. To restore the default, use the **service decimal-tty** command.

service decimal-tty

no service decimal-tty

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled (line numbers displayed as decimal numbers)

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

In the following example, the router is configured to display decimal rather than octal line numbers:

```
Router(config)# service decimal-tty
```

service exec-wait

To delay the startup of the EXEC on noisy lines, use the **service exec-wait** command in global configuration mode. To disable the delay function, use the **no** form of this command.

service exec-wait

no service exec-wait

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command delays startup of the EXEC until the line has been idle (no traffic seen) for 3 seconds. The default is to enable the line immediately on modem activation.

This command is useful on noisy modem lines or when a modem attached to the line is configured to ignore MNP/V.42 negotiations, and MNP/V.42 modems may be dialing in. In these cases, noise or MNP/V.42 packets may be interpreted as usernames and passwords, causing authentication failure before the user has a chance to type a username or password. The command is not useful on nonmodem lines or lines without some kind of login configured.

Examples

The following example delays the startup of the EXEC:

```
Router(config)# service exec-wait
```

service finger

The **service finger** command has been replaced by the **ip finger** command. However, the **service finge**r and **no service finger** commands continue to function to maintain backward compatibility with older versions of Cisco IOS software. Support for this command may be removed in a future release. See the description of the **ip finger** command for more information.

service hide-telnet-address

To hide addresses while trying to establish a Telnet session, use the **service hide-telnet-address** command in global configuration mode. To disable this service, use the **no** form of this command.

service hide-telnet-address

no service hide-telnet-address

Syntax Description

This command has no arguments or keywords.

Defaults

Addresses are displayed.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

When you attempt to connect to a device, the router displays addresses and other messages (for example, "Trying router1 (171.69.1.154, 2008)...)." With the hide feature, the router suppresses the display of the address (for example, "Trying router1 address #1..."). The router continues to display all other messages that would normally be displayed during a connection attempt, such as detailed error messages if the connection was not successful.

The hide feature improves the functionality of the busy-message feature. When you configure only the **busy-message** command, the normal messages generated during a connection attempt are not displayed; only the busy-message is displayed. When you use the hide and busy features together you can customize the information displayed during Telnet connection attempts. When you configure the **service hide-telnet-address** command and the **busy-message** command, the router suppresses the address and displays the message specified with the **busy-message** command if the connection attempt is not successful.

Examples

The following example hides Telnet addresses:

```
Router(config)# service hide-telnet-address
```

Related Commands

Command	Description
busy-message	Creates a "host failed" message that is displayed when a connection fails.

service linenumber

To configure the Cisco IOS software to display line number information after the EXEC or incoming banner, use the **service linenumber** command in global configuration mode. To disable this function, use the **no** form of this command.

service linenumber

no service linenumber

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

With the **service linenumber** command, you can have the Cisco IOS software display the host name, line number, and location each time an EXEC process is started, or an incoming connection is made. The line number banner appears immediately after the EXEC banner or incoming banner. This feature is useful for tracking problems with modems, because the host and line for the modem connection are listed. Modem type information can also be included.

Examples

In the following example, a user Telnets to Router2 before and after the **service linenumber** command is enabled. The second time, information about the line is displayed after the banner.

```
Router1> telnet Router2

Trying Router2 (172.30.162.131)... Open

Welcome to Router2.

User Access Verification

Password:
Router2> enable
Password:
Router2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)# service linenumber
Router2(config)# end
Router2# logout

[Connection to Router2 closed by foreign host]
Router1> telnet Router2
```

```
Trying Router2 (172.30.162.131)... Open

Welcome to Router2.

Router2 line 10


User Access Verification

Password:
Router2>
```

Related Commands

Command	Description
show users	Displays information about the active lines on the router.

service nagle

To enable the Nagle congestion control algorithm, use the **service nagle** command in global configuration mode. To to disable the algorithm, use the **no** form of this command.

service nagle

no service nagle

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When using a standard TCP implementation to send keystrokes between machines, TCP tends to send one packet for each keystroke typed. On larger networks, many small packets use up bandwidth and contribute to congestion.

The algorithm developed by John Nagle (RFC 896) helps alleviate the small-packet problem in TCP. In general, it works this way: The first character typed after connection establishment is sent in a single packet, but TCP holds any additional characters typed until the receiver acknowledges the previous packet. Then the second, larger packet is sent, and additional typed characters are saved until the acknowledgment comes back. The effect is to accumulate characters into larger chunks, and pace them out to the network at a rate matching the round-trip time of the given connection. This method is usually effective for all TCP-based traffic. However, do not use the **service nagle** command if you have XRemote users on X Window system sessions.

Examples

The following example enables the Nagle algorithm:

```
Router(config)# service nagle
```

service prompt config

To display the configuration prompt (config), use the **service prompt config** command in global configuration mode. To remove the configuration prompt, use the **no** form of this command.

service prompt config

no service prompt config

Syntax Description

This command has no arguments or keywords.

Defaults

The configuration prompts appear in all configuration modes.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Examples

In the following example, the **no service prompt config** command prevents the configuration prompt from being displayed. The prompt is still displayed in EXEC mode. When the **service prompt config** command is entered, the configuration mode prompt reappears.

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# no service prompt config
hostname newname
end
newname# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
service prompt config
newname(config)# hostname Router
Router(config)# end
Router#
```

Related Commands

Command	Description
hostname	Specifies or modifies the host name for the network server.
prompt	Customizes the prompt.

service sequence-numbers

To enable visible sequence numbering of system logging messages, use the **service sequence-numbers** command in global configuration mode. To disable visible sequence numbering of logging messages, use the **no** form of this command.

service sequence-numbers

no service sequence-numbers

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Each system status messages logged in the system logging process have a sequence reference number applied. This command makes that number visible by displaying it with the message. The sequence number is displayed as the first part of the system status message. See the description of the **logging** commands for information on displaying logging messages.

Examples

In the following example logging message sequence numbers are enabled:

```
.Mar 22 15:28:02 PST: %SYS-5-CONFIG_I: Configured from console by console
Router# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# service sequence-numbers
Router(config)# end
Router#
000066: .Mar 22 15:35:57 PST: %SYS-5-CONFIG_I: Configured from console by console
```

Related Commands

Command	Description
logging on	Enables system logging globally.
service timestamps	Enables time-stamping of system logging messages or debugging messages.

service slave-log

To allow slave Versatile Interface Processor (VIP) cards to log important error messages to the console, use the **service slave-log** command in global configuration mode. To disable slave logging, use the **no** form of this command.

service slave-log

no service slave-log

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command allows slave slots to log error messages of level 2 or higher (critical, alerts, and emergencies).

Examples

In the following example, the router is configured to log important messages from the slave cards to the console:

```
Router(config)# service slave-log
```

The following is sample output generated when this command is enabled:

```
%IPC-5-SLAVELOG: VIP-SLOT2:
 IPC-2-NOMEM: No memory available for IPC system initialization
```

The first line indicates which slot sent the message. The second line contains the error message.

service tcp-keepalives-in

To generate keepalive packets on idle incoming network connections (initiated by the remote host), use the **service tcp-keepalives-in** command in global configuration mode. To disable the keepalives, use the **no** form of this command.

service tcp-keepalives-in

no service tcp-keepalives-in

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

In the following example, keepalives on incoming TCP connections are generated:

```
Router(config)# service tcp-keepalives-in
```

Related Commands

Command	Description
service tcp-keepalives-out	Generates keepalive packets on idle outgoing network connections (initiated by a user).

service tcp-keepalives-out

To generate keepalive packets on idle outgoing network connections (initiated by a user), use the **service tcp-keepalives-out** command in global configuration mode. To disable the keepalives, use the **no** form of this command.

service tcp-keepalives-out

no service tcp-keepalives-out

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

In the following example, keepalives on outgoing TCP connections are generated:

```
Router(config)# service tcp-keepalives-out
```

Related Commands

Command	Description
service tcp-keepalives-in	Generates keepalive packets on idle incoming network connections (initiated by the remote host).

service tcp-small-servers

To access minor TCP/IP services available from hosts on the network, use the **service tcp-small-servers** command in global configuration mode. To disable these services, use the **no** form of the command.

service tcp-small-servers

no service tcp-small-servers

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

By default, the TCP servers for Echo, Discard, Chargen, and Daytime services are disabled.

When the minor TCP/IP servers are disabled, access to the Echo, Discard, Chargen, and Daytime ports cause the Cisco IOS software to send a TCP RESET packet to the sender and discard the original incoming packet.

Note Unlike defaults for other commands, this command will be displayed when you use the **show running config** command to display current settings whether or not you have changed the default using the **no service tcp-small-servers** command.

Examples

The following example enables minor TCP/IP services available from the network:

```
Router(config)# service tcp-small-servers
```

service telnet-zero-idle

To set the TCP window to zero (0) when the Telnet connection is idle, use the **service telnet-zero-idle** command in global configuration mode. To disable this service, use the **no** form of this command.

service telnet-zero-idle

no service telnet-zero-idle

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Normally, data sent to noncurrent Telnet connections is accepted and discarded. When the **service telnet-zero-idle** command is enabled, if a session is suspended (that is, some other connection is made active or the EXEC is sitting in command mode), the TCP window is set to zero. This action prevents the remote host from sending any more data until the connection is resumed. Use this command when it is important that all messages sent by the host be seen by the users and the users are likely to use multiple sessions.

Do not use this command if your host will eventually time out and log out a TCP user whose window is zero.

Examples

The following example sets the TCP window to zero when the Telnet connection is idle:

```
Router(config)# service telnet-zero-idle
```

Related Commands

Command	Description
resume	Switches to another open Telnet, rlogin, LAT, or PAD session.

service timestamps

To configure the system to time-stamp debugging or system logging messages, use one of the **service timestamps** commands in global configuration mode. To disable this service, use the **no** form of this command.

service timestamps {**debug** | **log**} **uptime**

service timestamps {**debug** | **log**} **datetime** [**msec**] [**localtime**] [**show-timezone**] [**year**]

no service timestamps [**debug** | **log**]

Syntax Description

debug	Indicates that the timestamp should be applied to debugging messages.
log	Indicates that the timestamp should be applied to system logging messages.
uptime	Time stamp with the time since the system was rebooted. The time stamp format for uptime is HHHH:MM:SS.
datetime	Time stamp with the date and time. The time stamp format for datetime is MMM DD HH:MM:SS.
msec	(Optional) Include milliseconds in the time stamp.
localtime	(Optional) Time stamp relative to the local time zone.
year	Include the year in the datetime format.
show-timezone	(Optional) Include the time zone name in the time stamp.

Defaults

No time-stamping.

If the **service timestamps** command is specified with no arguments or keywords, the default is **service timestamps debug uptime**.

The default for the **service timestamps** *type* **datetime** command is to format the time in Coordinated Universal Time (UTC), with no milliseconds and no time zone name.

The **no service timestamps** command by itself disables time stamps for both debug and log messages.

To set the local timezone, use the **clock timezone** *zone hours-offset* command in global configuration mode.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(15)T	The **year** keyword was added.

Usage Guidelines

Time stamps can be added to either debugging or logging messages independently. The **uptime** form of the command adds time stamps in the format HHHH:MM:SS, indicating the time since the system was rebooted. The **datetime** form of the command adds time stamps in the format MMM DD HH:MM:SS, indicating the date and time according to the system clock.

The timestamp will be preceeded by an asterisk or period if the time is potentially inaccurate. Table 43 describes the symbols that proceed the timestamp.

Table 43 Timestamping Symbols for syslog Messages

Symbol	Description	Example
(blank)	Time is authoritative: the software clock is in sync or has just been set manually	15:29:03.158 UTC Tue Feb 25 2003:
*	Time is not authoritative: the software clock has not been set, or is not in sync with configured Network Time Protocol (NTP) servers.	*15:29:03.158 UTC Tue Feb 25 2003:
.	Time is authoritative, but the Network Time Protocol (NTP) is not synchronized: the software clock was in sync, but has since lost contact with all configured NTP servers.	.15:29:03.158 UTC Tue Feb 25 2003:

Examples

In the following example, the user enables time stamps on debugging messages, showing the time since reboot:

```
service timestamps debug uptime
```

In the following example, the user enables time stamps on logging messages, showing the current time and date relative to the local time zone, with the time zone name included:

```
Router(config)#
! The following line shows timestamp with uptime.
1w0d: %SYS-5-CONFIG_I: Configured from console by console
Router(config)# service timestamps log datetime localtime show-timezone
Router(config)# end
Router#
! The following line shows timestamp with datetime.
.Mar 22 23:13:25 UTC: %SYS-5-CONFIG_I: Configured from console by console
```

The following example shows the change from UTC to local time:

```
Router#
.Mar 22 23:23:10 UTC: %SYS-5-CONFIG_I: Configured from console by console
Router# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# clock timezone PST -8
Router(config)# end
Router#
.Mar 22 15:28:02 PST: %SYS-5-CONFIG_I: Configured from console by console
```

Related Commands

Command	Description
clock set	Manually sets the system clock.
ntp	Controls access to the system's NTP services.
service sequence-numbers	Stamps system logging messages with a sequence number.

service udp-small-servers

To access minor User Datagram Protocol (UDP) services available from hosts on the network, use the **service udp-small-servers** command in global configuration mode. To disable these services, use the **no** form of this command.

service udp-small-servers

no service udp-small-servers

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

By default the UPD servers for Echo, Discard, and Chargen services are disabled.

When the servers are disabled, access to Echo, Discard, and Chargen ports causes the Cisco IOS software to send an "ICMP port unreachable" message to the sender and discard the original incoming packet.

Examples

In the following example, the UDP server (UDP services) is enabled:

```
Router(config)# service udp-small-servers
```

setup

To enter Setup mode, use the **setup** command in privileged EXEC mode.

setup

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Setup mode gives you the option of configuring your system without using the Cisco IOS Command Line Interface (CLI). For some tasks, you may find it easier to use Setup than to enter Cisco IOS commands individually. For example, you might want to use Setup to add a protocol suite, to make major addressing scheme changes, or to configure a newly installed interface. Although you can use the CLI to make these changes, Setup provides you with a high-level view of the configuration and guides you through the configuration process.

If you are not familiar with Cisco products and the CLI, Setup is a particularly valuable tool because it prompts you for the specific information required to configure your system.

Note If you use the Setup mode to modify a configuration because you have added or modified the hardware, be sure to verify the physical connections using the **show version** EXEC command. Also, verify the logical port assignments using the **show running-config** EXEC command to ensure that you configure the correct port. Refer to the hardware documentation for your platform for more information on physical and logical port assignments.

Before using the Setup mode, you should have the following information so that you can configure the system properly:

- Which interfaces you want to configure
- Which routing protocols you wish to enable
- Whether the router is to perform bridging
- Network addresses for the protocols being configured
- Password strategy for your environment

When you enter the **setup** EXEC command after first-time startup, an interactive dialog called the *System Configuration Dialog* appears on the system console screen. The System Configuration Dialog guides you through the configuration process. It prompts you first for global parameters and then for interface parameters. The values shown in brackets next to each prompt reflect either the default settings or the last configured setting.

The prompts and the order in which they appear on the screen vary depending on the platform and the interfaces installed in the device.

You must progress through the System Configuration Dialog until you come to the item that you intend to change. To accept default settings for items that you do not want to change, press the **Return** or **Enter** key. The default choice is indicated by square brackets (for example, [yes]) before the prompt colon (:).

To exit Setup mode and return to privileged EXEC mode without making changes and without progressing through the entire System Configuration Dialog, press **Ctrl-C**.

The facility also provides help text for each prompt. To access help text, press the question mark (**?**) key at a prompt.

When you complete your changes, the system will automatically display the configuration file that was created during the Setup session. It also asks you if you want to use this configuration. If you answer Yes, the configuration is saved to NVRAM as the startup configuration file. If you answer No, the configuration is not saved and the process begins again. There is no default for this prompt; you must answer either Yes or No.

Examples

The following example displays the **setup** command facility to configure serial interface 0 and to add ARAP and IP/IPX PPP support on the asynchronous interfaces:

```
Router# setup

         --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Continue with configuration dialog? [yes]:

First, would you like to see the current interface summary? [yes]:

Interface          IP-Address      OK?  Method    Status                  Protocol
Ethernet0          172.16.72.2     YES  manual    up                      up
Serial0            unassigned      YES  not set   administratively down  down
Serial1            172.16.72.2     YES  not set   up                      up

Configuring global parameters:

  Enter host name [Router]:

The enable secret is a one-way cryptographic secret used
instead of the enable password when it exists.

  Enter enable secret [<Use current secret>]:


The enable password is used when there is no enable secret
and when using older software and some boot images.


  Enter enable password [ww]:
  Enter virtual terminal password [ww]:
  Configure SNMP Network Management? [yes]:
    Community string [public]:
  Configure DECnet? [no]:
  Configure AppleTalk? [yes]:
    Multizone networks? [no]: yes
  Configure IPX? [yes]:
  Configure IP? [yes]:
    Configure IGRP routing? [yes]:
      Your IGRP autonomous system number [15]:
```

```
  Configure Async lines? [yes]:
    Async line speed [9600]: 57600
    Configure for HW flow control? [yes]:
    Configure for modems? [yes/no]: yes
      Configure for default chat script? [yes]: no
    Configure for Dial-in IP SLIP/PPP access? [no]: yes
      Configure for Dynamic IP addresses? [yes]: no
      Configure Default IP addresses? [no]: yes
      Configure for TCP Header Compression? [yes]: no
      Configure for routing updates on async links? [no]:
    Configure for Async IPX? [yes]:
    Configure for Appletalk Remote Access? [yes]:
      AppleTalk Network for ARAP clients [1]: 20
      Zone name for ARAP clients [ARA Dialins]:

Configuring interface parameters:

Configuring interface Ethernet0:
  Is this interface in use? [yes]:
  Configure IP on this interface? [yes]:
    IP address for this interface [172.16.72.2]:
    Number of bits in subnet field [8]:
    Class B network is 172.16.0.0, 8 subnet bits; mask is /24
  Configure AppleTalk on this interface? [yes]:
    Extended AppleTalk network? [yes]:
    AppleTalk starting cable range [1]:
    AppleTalk ending cable range [1]:
    AppleTalk zone name [Sales]:
    AppleTalk additional zone name:
  Configure IPX on this interface? [yes]:
    IPX network number [1]:

Configuring interface Serial0:
  Is this interface in use? [no]: yes
  Configure IP on this interface? [no]: yes
  Configure IP unnumbered on this interface? [no]: yes
    Assign to which interface [Ethernet0]:
  Configure AppleTalk on this interface? [no]: yes
    Extended AppleTalk network? [yes]:
    AppleTalk starting cable range [2]: 3
    AppleTalk ending cable range [3]: 3
    AppleTalk zone name [myzone]: ZZ Serial
    AppleTalk additional zone name:
  Configure IPX on this interface? [no]: yes
    IPX network number [2]: 3

Configuring interface Serial1:
  Is this interface in use? [yes]:
  Configure IP on this interface? [yes]:
  Configure IP unnumbered on this interface? [yes]:
    Assign to which interface [Ethernet0]:
  Configure AppleTalk on this interface? [yes]:
    Extended AppleTalk network? [yes]:
    AppleTalk starting cable range [2]:
    AppleTalk ending cable range [2]:
    AppleTalk zone name [ZZ Serial]:
    AppleTalk additional zone name:
  Configure IPX on this interface? [yes]:
    IPX network number [2]:
Configuring interface Async1:
    IPX network number [4]:
    Default client IP address for this interface [none]: 172.16.72.4
Configuring interface Async2:
    IPX network number [5]:
```

```
    Default client IP address for this interface [172.16.72.5]:
Configuring interface Async3:
    IPX network number [6]:
    Default client IP address for this interface [172.16.72.6]:
Configuring interface Async4:
    IPX network number [7]:
    Default client IP address for this interface [172.16.72.7]:
Configuring interface Async5:
    IPX network number [8]:
    Default client IP address for this interface [172.16.72.8]:
Configuring interface Async6:
    IPX network number [9]:
    Default client IP address for this interface [172.16.72.9]:
Configuring interface Async7:
    IPX network number [A]:
    Default client IP address for this interface [172.16.72.10]:
Configuring interface Async8:
    IPX network number [B]:
    Default client IP address for this interface [172.16.72.11]:
Configuring interface Async9:
    IPX network number [C]:
    Default client IP address for this interface [172.16.72.12]:
Configuring interface Async10:
    IPX network number [D]:
    Default client IP address for this interface [172.16.72.13]:
Configuring interface Async11:
    IPX network number [E]:
    Default client IP address for this interface [172.16.72.14]:
Configuring interface Async12:
    IPX network number [F]:
    Default client IP address for this interface [172.16.72.15]:
Configuring interface Async13:
    IPX network number [10]:
    Default client IP address for this interface [172.16.72.16]:
Configuring interface Async14:
    IPX network number [11]:
    Default client IP address for this interface [172.16.72.17]:
Configuring interface Async15:
    IPX network number [12]:
    Default client IP address for this interface [172.16.72.18]:
Configuring interface Async16:
    IPX network number [13]:
    Default client IP address for this interface [172.16.72.19]:

The following configuration command script was created:

hostname Router
enable secret 5 $1$krIg$emfYm/1OwHVspDuS8Gy0K1
enable password ww
line vty 0 4
password ww
snmp-server community public
!
no decnet routing
appletalk routing
ipx routing
ip routing
!
line 1 16
speed 57600
flowcontrol hardware
modem inout
!
arap network 20 ARA Dialins
```

```
line 1 16
arap enable
autoselect
!
! Turn off IPX to prevent network conflicts.
interface Ethernet0
no ipx network
interface Serial0
no ipx network
interface Serial1
no ipx network
!
interface Ethernet0
ip address 172.16.72.2 255.255.255.0
appletalk cable-range 1-1 1.204
appletalk zone Sales
ipx network 1
no mop enabled
!
interface Serial0
no shutdown
no ip address
ip unnumbered Ethernet0
appletalk cable-range 3-3
appletalk zone ZZ Serial
ipx network 3
no mop enabled
!
interface Serial1
no ip address
ip unnumbered Ethernet0
appletalk cable-range 2-2 2.2
appletalk zone ZZ Serial
ipx network 2
no mop enabled
!
Interface Async1
ipx network 4
ip unnumbered Ethernet0
peer default ip address 172.16.72.4
async mode interactive
!
Interface Async2
ipx network 5
ip unnumbered Ethernet0
peer default ip address 172.16.72.5
async mode interactive
!
Interface Async3
ipx network 6
ip unnumbered Ethernet0
peer default ip address 172.16.72.6
async mode interactive
!
Interface Async4
ipx network 7
ip unnumbered Ethernet0
peer default ip address 172.16.72.7
async mode interactive
async dynamic address
!
Interface Async5
ipx network 8
ip unnumbered Ethernet0
```

```
peer default ip address 172.16.72.8
async mode interactive
!
Interface Async6
ipx network 9
ip unnumbered Ethernet0
peer default ip address 172.16.72.9
async mode interactive
!
Interface Async7
ipx network A
ip unnumbered Ethernet0
peer default ip address 172.16.72.10
async mode interactive
!
Interface Async8
ipx network B
ip unnumbered Ethernet0
peer default ip address 172.16.72.11
async mode interactive
!
Interface Async9
ipx network C
ip unnumbered Ethernet0
peer default ip address 172.16.72.12
async mode interactive
!
Interface Async10
ipx network D
ip unnumbered Ethernet0
peer default ip address 172.16.72.13
async mode interactive
!
Interface Async11
ipx network E
ip unnumbered Ethernet0
peer default ip address 172.16.72.14
async mode interactive
!
Interface Async12
ipx network F
ip unnumbered Ethernet0
peer default ip address 172.16.72.15
async mode interactive
!
Interface Async13
ipx network 10
ip unnumbered Ethernet0
peer default ip address 172.16.72.16
async mode interactive
!
Interface Async14
ipx network 11
ip unnumbered Ethernet0
peer default ip address 172.16.72.17
async mode interactive
!
Interface Async15
ipx network 12
ip unnumbered Ethernet0
peer default ip address 172.16.72.18
async mode interactive
!
Interface Async16
```

```
ipx network 13
ip unnumbered Ethernet0
peer default ip address 172.16.72.19
async mode interactive
!
router igrp 15
network 172.16.0.0
!
end

Use this configuration? [yes/no]: yes

Building configuration...

Use the enabled mode 'configure' command to modify this configuration.

Router#
```

Related Commands

Command	Description
erase nvram:	Erases a file system.
show running-config	Displays the running configuration file. Command alias for the **more system:running-config** command.
show startup-config	Displays the startup configuration file. Command alias for the **more system:startup-config** command.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

show aliases

To display all alias commands, or the alias commands in a specified mode, use the **show aliases** command in EXEC mode.

show aliases [*mode*]

Syntax Description

mode	(Optional) Name of a specific command or configuration mode. Specifies that only aliases configured for this mode should be displayed.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

When used without the *mode* argument, this command will display all aliases currently configured on the system. Use the *mode* argument to display only the aliases configured for the specified command mode.

To display a list of the command mode keywords available for your system, use the **show aliases ?** command. For a list of command modes, refer to the "Cisco IOS Command Modes" appendix in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Examples

The following is sample output from the **show aliases exec** commands. The aliases configured for commands in EXEC mode are displayed.

```
Router> show aliases exec

Exec mode aliases:
  h                    help
  lo                   logout
  p                    ping
  r                    resume
  s                    show
  w                    where
```

Related Commands

Command	Description
alias	Creates a command alias.

show async bootp

To display the extended BOOTP request parameters that have been configured for asynchronous interfaces, use the **show async bootp** command in privileged EXEC mode.

show async bootp

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample output from the **show async bootp** command:

```
Router# show async bootp

The following extended data will be sent in BOOTP responses:

bootfile (for address 192.168.1.1) "pcboot"
bootfile (for address 172.16.1.111) "dirtboot"
subnet-mask 255.255.0.0
time-offset -3600
time-server 192.168.1.1
```

Table 44 describes the significant fields shown in the display.

Table 44 show async bootp Field Descriptions

Field	Description
bootfile... "pcboot"	Boot file for address 192.168.1.1 is named pcboot.
subnet-mask 255.255.0.0	Subnet mask.
time-offset -3600	Local time is one hour (3600 seconds) earlier than UTC time.
time-server 192.168.1.1	Address of the time server for the network.

Related Commands

Command	Description
async-bootp	Configures extended BOOTP requests for asynchronous interfaces as defined in RFC 1084.

show bootvar

To display the contents of the BOOT variable, the name of the configuration file pointed to by the CONFIG_FILE variable, the contents of the BOOTLDR variable, and the configuration register setting, use the **show bootvar** command in EXEC mode.

show bootvar

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.

Usage Guidelines

The **show bootvar** command replaces the **show boot** command.

The **show bootvar** command allows you to view the current settings for the following variables:

- BOOT
- CONFIG_FILE
- BOOTLDR

The BOOT variable specifies a list of bootable images on various devices. The CONFIG_FILE variable specifies the configuration file used during system initialization. The BOOTLDR variable specifies the Flash device and filename containing the rxboot image that ROM uses for booting. You set these variables with the **boot system**, **boot config**, and **boot bootldr** global configuration commands, respectively.

When you use this command on a device with multiple RSP cards (Dual RSPs), this command also shows you the variable settings for both the master and slave RSP card.

Examples

The following is sample output from the **show bootvar** command:

```
Router# show bootvar

BOOT variable =
CONFIG_FILE variable = nvram:
Current CONFIG_FILE variable = slot0:router-config
BOOTLDR variable not exist

Configuration register is 0x0

Router#
```

In the sample output, the BOOT variable contains a null string. That is, a list of bootable images is not specified.

The CONFIG_FILE variable points to the configuration file in NVRAM as the startup (initialization) configuration. The run-time value for the CONFIG_FILE variable points to the router-config file on the Flash memory card inserted in the first slot of the RSP card. That is, during the run-time configuration, you have modified the CONFIG_FILE variable using the **boot config** command, but you have not saved the run-time configuration to the startup configuration. To save your run-time configuration to the startup configuration, use the **copy system:running-config nvram:startup-config** command. If you do not save the run-time configuration to the startup configuration, then the system reverts to the saved CONFIG_FILE variable setting for initialization information upon reload. In this sample, the system reverts to NVRAM for the startup configuration file.

The BOOTLDR variable does not yet exist. That is, you have not created the BOOTLDR variable using the **boot bootldr** global configuration command.

The following example is output from the **show bootvar** command for a Cisco 7513 router configured for HSA:

```
Router# show bootvar

BOOT variable =
CONFIG_FILE variable =
Current CONFIG_FILE variable =
BOOTLDR variable does not exist

Configuration register is 0x0

current slave is in slot 7
BOOT variable =
CONFIG_FILE variable =
BOOTLDR variable does not exist

Configuration register is 0x0

Router#
```

Related Commands

Command	Description
boot bootstrap	Configures the filename that is used to boot a secondary bootstrap image.
boot config	Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).
boot system	Specifies the system image that the router loads at startup.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

show buffers

To display statistics for the buffer pools on the network server, use the **show buffers** command in EXEC mode.

show buffers [{**address** *hex-address* | **failures** | **pool** *pool-name* | {**all** | **assigned** | **free** | **old** | **input-interface** *interface-type interface-number*} [**pool** *pool-name*]} [**dump** | **header** | **packet**]]

Syntax Description

address *hex-address*	(Optional) Displays buffers at a specified address. Specify address in hexadecimal notation.
failures	(Optional) Displays buffer allocation failures.
pool *pool-name*	(Optional) Displays buffers in a specified buffer pool.
all	(Optional) Displays all buffers.
assigned	(Optional) Displays the buffers in use.
free	(Optional) Displays the buffers available for use.
old	(Optional) Displays buffers older than one minute.
input-interface *interface-type interface-number*	(Optional) Displays interface pool information. If an interface type is specified and this interface has its own buffer pool, information for that pool is displayed.
dump	(Optional) Displays the buffer header and all data.
header	(Optional) Displays the buffer header only.
packet	(Optional) Displays the buffer header and packet data.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.3	The option to filter display output based on specific buffer pools was expanded.

Examples

The following is sample output from the **show buffers** command with no arguments, showing all buffer pool information:

```
Router> show buffers

Buffer elements:
     398 in free list (500 max allowed)
     1266 hits, 0 misses, 0 created

Public buffer pools:
Small buffers, 104 bytes (total 50, permanent 50):
     50 in free list (20 min, 150 max allowed)
     551 hits, 0 misses, 0 trims, 0 created
Middle buffers, 600 bytes (total 25, permanent 25):
```

```
     25 in free list (10 min, 150 max allowed)
     39 hits, 0 misses, 0 trims, 0 created
Big buffers, 1524 bytes (total 50, permanent 50):
     49 in free list (5 min, 150 max allowed)
     27 hits, 0 misses, 0 trims, 0 created
VeryBig buffers, 4520 bytes (total 10, permanent 10):
     10 in free list (0 min, 100 max allowed)
     0 hits, 0 misses, 0 trims, 0 created
Large buffers, 5024 bytes (total 0, permanent 0):
     0 in free list (0 min, 10 max allowed)
     0 hits, 0 misses, 0 trims, 0 created
Huge buffers, 18024 bytes (total 0, permanent 0):
     0 in free list (0 min, 4 max allowed)
     0 hits, 0 misses, 0 trims, 0 created

Interface buffer pools:
Ethernet0 buffers, 1524 bytes (total 64, permanent 64):
     16 in free list (0 min, 64 max allowed)
     48 hits, 0 fallbacks
     16 max cache size, 16 in cache
Ethernet1 buffers, 1524 bytes (total 64, permanent 64):
     16 in free list (0 min, 64 max allowed)
     48 hits, 0 fallbacks
     16 max cache size, 16 in cache
Serial0 buffers, 1524 bytes (total 64, permanent 64):
     16 in free list (0 min, 64 max allowed)
     48 hits, 0 fallbacks
     16 max cache size, 16 in cache
Serial1 buffers, 1524 bytes (total 64, permanent 64):
     16 in free list (0 min, 64 max allowed)
     48 hits, 0 fallbacks
     16 max cache size, 16 in cache
TokenRing0 buffers, 4516 bytes (total 48, permanent 48):
     0 in free list (0 min, 48 max allowed)
     48 hits, 0 fallbacks
     16 max cache size, 16 in cache
TokenRing1 buffers, 4516 bytes (total 32, permanent 32):
     32 in free list (0 min, 48 max allowed)
     16 hits, 0 fallbacks

0 failures (0 no memory)
```

Table 45 describes the significant fields shown in the display.

Table 45 show buffers Field Descriptions

Field	Description
Buffer elements	Small structures used as placeholders for buffers in internal operating system queues. Used when a buffer may need to be on more than one queue.
free list	Total number of the currently unallocated buffer elements.
max allowed	Maximum number of buffers that are available for allocation.
hits	Count of successful attempts to allocate a buffer when needed.
misses	Count of buffer allocation attempts that resulted in growing the buffer pool to allocate a buffer.
created	Count of new buffers created to satisfy buffer allocation attempts when the available buffers in the pool have already been allocated.
Public buffer pools:	

Table 45 show buffers Field Descriptions (continued)

Field	Description
Small buffers	Buffers that are 104 bytes long.
Middle buffers	Buffers that are 600 bytes long.
Big buffers	Buffers that are 1524 bytes long.
VeryBig buffers	Buffers that are 4520 bytes long.
Large buffers	Buffers that are 5024 bytes long.
Huge buffers	Buffers that are 18024 bytes long.
total	Total number of this type of buffer.
permanent	Number of these buffers that are permanent.
free list	Number of available or unallocated buffers in that pool.
min	Minimum number of free or unallocated buffers in the buffer pool.
max allowed	Maximum number of free or unallocated buffers in the buffer pool.
hits	Count of successful attempts to allocate a buffer when needed.
misses	Count of buffer allocation attempts that resulted in growing the buffer pool in order to allocate a buffer.
trims	Count of buffers released to the system because they were not being used. This field is displayed only for dynamic buffer pools, not interface buffer pools, which are static.
created	Count of new buffers created in response to misses. This field is displayed only for dynamic buffer pools, not interface buffer pools, which are static.
Interface buffer pools:	
total	Total number of this type of buffer.
permanent	Number of these buffers that are permanent.
free list	Number of available or unallocated buffers in that pool.
min	Minimum number of free or unallocated buffers in the buffer pool.
max allowed	Maximum number of free or unallocated buffers in the buffer pool.
hits	Count of successful attempts to allocate a buffer when needed.
fallbacks	Count of buffer allocation attempts that resulted in falling back to the public buffer pool that is the smallest pool at least as big as the interface buffer pool.
max cache size	Maximum number of buffers from the pool of that interface that can be in the buffer pool cache of that interface. Each interface buffer pool has its own cache. These are not additional to the permanent buffers; they come from the buffer pools of the interface. Some interfaces place all of their buffers from the interface pool into the cache. In this case, it is normal for the *free list* to display 0.
failures	Total number of allocation requests that have failed because no buffer was available for allocation; the datagram was lost. Such failures normally occur at interrupt level.
no memory	Number of failures that occurred because no memory was available to create a new buffer.

The following is sample output from the **show buffers** command with an interface type and number identifier:

```
Router> show buffers input-interface Ethernet 0

Ethernet0 buffers, 1524 bytes (total 64, permanent 64):
     16 in free list (0 min, 64 max allowed)
     48 hits, 0 fallbacks
     16 max cache size, 16 in cache
```

show c2600

To display information for troubleshooting the Cisco 2600 series router, use the **show c2600** command in EXEC mode.

show c2600

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3 XA	This command was introduced.

Usage Guidelines

The **show c2600** command provides complex troubleshooting information that pertains to the platform's shared references rather than to a specific interface.

Examples

The following is sample output from the **show c2600** command:

```
Router# show c2600

C2600 Platform Information:
Interrupts:

 Assigned Handlers...
  Vect  Handler   # of Ints   Name
    00  801F224C   00000000   Xilinx bridge error interrupt
    01  801DE768   0D3EE155   MPC860 TIMER INTERRUPT
    02  801E94E0   0000119E   16552 Con/Aux Interrupt
    04  801F0D94   00000000   PA Network Management Int Handler
    05  801E6C34   00000000   Timebase Reference Interrupt
    06  801F0DE4   00002C1A   PA Network IO Int Handler
    07  801F0EA0   0000015D   MPC860 CPM INTERRUPT
    14  801F224C   00000000   Xilinx bridge error interrupt

 IOS Priority Masks...
  Level 00 = [ EF020000 ]
  Level 01 = [ EC020000 ]
  Level 02 = [ E8020000 ]
  Level 03 = [ E0020000 ]
  Level 04 = [ E0020000 ]
  Level 05 = [ E0020000 ]
  Level 06 = [ C0020000 ]
  Level 07 = [ 00000000 ]

 SIU_IRQ_MASK  = FFFFFFFF  SIEN   = EF02xxxx   Current Level = 00
 Spurious IRQs = 00000000  SIPEND = 0000xxxx

 Interrupt Throttling:
  Throttle Count = 00000000   Timer Count      = 00000000
```

```
  Netint usec    = 00000000   Netint Mask usec = 000003E8
  Active         =        0   Configured       =        0
  Longest IRQ    = 00000000

IDMA Status:
 Requests = 00000349      Drops                = 00000000
 Complete = 00000349      Post Coalesce Frames = 00000349
 Giant    = 00000000
 Available Blocks = 256/256

ISP Status:
 Version string burned in chip: "A986122997"
 New version after next program operation: "B018020998"
 ISP family type: "2096"
 ISP chip ID: 0x0013
 Device is  programmable
```

Table 46 describes the significant fields shown in the display.

Table 46 show c2600 Field Descriptions

Field	Description
Interrupts	Denotes that the next section describes the status of the interrupt services.
Assigned Handlers	Denotes a subsection of the Interrupt section that displays data about the interrupt handlers.
Vect	The processor vector number.
Handler	The execution address of the handler assigned to this vector.
# of Ints	The number of times this handler has been called.
Name	The name of the handler assigned to this vector.
IOS Priority Masks	Denotes the subsection of the Interrupt section that displays internal Cisco IOS priorities. Each item in this subsection indicates a Cisco IOS interrupt level and the bit mask used to mask out interrupt sources when that Cisco IOS level is being processed. Used exclusively for debugging.
SIU_IRQ_MASK	For engineering level debug only.
Spurious IRQs	For engineering level debug only.
Interrupt Throttling:	This subsection describes the behavior of the Interrupt Throttling mechanism on the platform.
Throttle Count	Number of times throttle has become active.
Timer Count	Number of times throttle has deactivated because the maximum masked out time for network interrupt level has been reached.
Netint usec	Maximum time network level is allowed to run (in microseconds).
Netint Mask usec	Maximum time network level interrupt is masked out to allow process level code to run (in microseconds).
Active	Indicates that the network level interrupt is masked or that the router is in interrupt throttle state.
Configured	Indicates that throttling is enabled or configured when set to 1.
Longest IRQ	Duration of longest network level interrupt (in microseconds).

Table 46 show c2600 Field Descriptions (continued)

Field	Description
IDMA Status	Monitors the activity of the Internal Direct Memory Access (IDMA) hardware and software. Used to coalesce packets (turn particularized packets into non particularized packets) for transfer to the process level switching mechanism.
Requests	Number of times the IDMA engine is asked to coalesce a packet.
Drops	Number of times the coalescing operation was aborted.
Complete	Number of times the operation was successful.
Post Coalesce Frames	Number of Frames completed post coalesce processing.
Giant	Number of packets too large to coalesce.
Available Blocks	Indicates the status of the request queue, in the format N/M where N is the number of empty slots in queue and M is the total number of slots; for example, 2/256 indicates that the queue has 256 entries and can accept two more requests before it is full.
ISP Status	Provides status of In-System-Programmable (ISP) hardware.
Version string burned in chip	Current version of ISP hardware.
New version after next program operation	Version of ISP hardware after next ISP programming operation.
ISP family type	Device family number of ISP hardware.
ISP chip ID	Internal ID of ISP hardware as designated by the chip manufacturer.
Device is programmable	"Yes" or "No." Indicates if an ISP operation is possible on this board.

Related Commands

Command	Description
show context	Displays information stored in NVRAM when the router crashes.

show c7200

To display information about the CPU and midplane for Cisco 7200 series routers, use the **show c7200** command in EXEC mode.

show c7200

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

You can use the output of this command to determine whether the hardware version level and upgrade is current. The information is generally useful for diagnostic tasks performed by technical support only.

Examples

The following is sample output from the **show c7200** command:

```
Router# show c7200

C7200 Network IO Interrupt Throttling:
 throttle count=0, timer count=0
 active=0, configured=0
 netint usec=3999, netint mask usec=200

C7200 Midplane EEPROM:
        Hardware revision 1.2           Board revision A0
        Serial number     2863311530    Part number    170-43690-170
        Test history      0xAA          RMA number     170-170-170
        MAC=0060.3e28.ee00, MAC Size=1024
        EEPROM format version 1, Model=0x6
        EEPROM contents (hex):
          0x20: 01 06 01 02 AA AA AA AA AA AA AA AA 00 60 3E 28
          0x30: EE 00 04 00 AA AA AA AA AA AA AA 50 AA AA AA AA

C7200 CPU EEPROM:
        Hardware revision 2.0           Board revision A0
        Serial number     3509953       Part number     73-1536-02
        Test history      0x0           RMA number      00-00-00
        EEPROM format version 1
        EEPROM contents (hex):
          0x20: 01 15 02 00 00 35 8E C1 49 06 00 02 00 00 00 00
          0x30: 50 00 00 00 FF FF FF FF FF FF FF FF FF FF FF FF
```

show calendar

To display the current time and date setting for the hardware clock, use the **show calendar** command in EXEC mode:

show calendar

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Some platforms have a hardware clock (calendar) which is separate from the software clock. The hardware clock is battery operated, and runs continuously, even if the router is powered off or rebooted.

You can compare the time and date shown with this command with the time and date listed via the **show clock** EXEC command to verify that the hardware clock and software clock are synchronized with each other. The time displayed is relative to the configured time zone.

Examples

In the following sample display, the hardware clock indicates the time stamp of 12:13:44 p.m. on Friday, July 19, 1996:

```
Router> show calendar

12:13:44 PST Fri Jul 19 1996
```

Related Commands

Command	Description
show clock	Displays the time and date from the system software clock.

show cdp entry

To display information about a specific neighboring device discovered using Cisco Discovery Protocol (CDP), use the **show cdp entry** command in privileged EXEC mode.

show cdp entry {***** | *device-name*[*****] [**protocol** | **version**]}

Syntax Description

*****	Displays all of the CDP neighbors.
device-name	Name of the neighbor about which you want information.
*device-name******	You can enter an asterisk (*) at the end of an *entry-name* as a wildcard. For example, entering **show cdp entry dev*** will match all entries which begin with **dev**.
protocol	(Optional) Limits the display to information about the protocols enabled on a router.
version	(Optional) Limits the display to information about the version of software running on the router.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.

Examples

The following is sample output from the **show cdp entry** command with no limits. Information about the neighbor device.cisco.com is displayed, including device ID, address and protocol, platform, interface, hold time, and version.

```
Router# show cdp entry device.cisco.com

-------------------------
Device ID: device.cisco.com
Entry address(es):
  IP address: 192.168.68.18
  CLNS address: 490001.1111.1111.1111.00
  DECnet address: 10.1
Platform: cisco 4500,  Capabilities: Router
Interface: Ethernet0/1,  Port ID (outgoing port): Ethernet0
Holdtime : 125 sec

Version :
Cisco IOS Software
Cisco IOS (tm) 4500 Software (C4500-J-M), Version 12.1(2)
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Mon 07-Apr-00 19:51 by joeuser
```

The following is sample output from the **show cdp entry protocol** command. Only information about the protocols enabled on device.cisco.com is displayed.

```
Router# show cdp entry device.cisco.com protocol

Protocol information for device.cisco.com:
  IP address: 192.168.68.18
  CLNS address: 490001.1111.1111.1111.00
  DECnet address: 10.1
```

The following is sample output from the **show cdp entry version** command. Only information about the version of software running on *device.cisco.com* is displayed.

```
Router# show cdp entry device.cisco.com version

Version information for device.cisco.com:
  Cisco IOS Software
Cisco IOS (tm) 4500 Software (C4500-J-M), Version 12.1(2)
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Mon 07-Apr-00 19:51 by joeuser
```

Related Commands

Command	Description
show cdp	Displays global CDP information, including timer and hold-time information.
show cdp interface	Displays information about the interfaces on which CDP is enabled.
show cdp neighbors	Displays detailed information about neighboring devices discovered using CDP.
show cdp traffic	Displays traffic information from the CDP table.

show cdp interface

To display information about the interfaces on which Cisco Discovery Protocol (CDP) is enabled, use the **show cdp interface** command in privileged EXEC mode.

show cdp interface [*type number*]

Syntax Description

type	(Optional) Type of interface about which you want information.
number	(Optional) Number of the interface about which you want information.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.

Examples

The following is sample output from the **show cdp interface** command. Status information and information about CDP timer and hold-time settings is displayed for all interfaces on which CDP is enabled.

```
Router# show cdp interface

Serial0 is up, line protocol is up, encapsulation is SMDS
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Ethernet0 is up, line protocol is up, encapsulation is ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
```

The following is sample output from the **show cdp interface** command with an interface specified. Status information and information about CDP timer and hold-time settings is displayed for Ethernet interface 0 only.

```
Router# show cdp interface ethernet 0

Ethernet0 is up, line protocol is up, encapsulation is ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
```

Related Commands

Command	Description
show cdp	Displays global CDP information, including timer and hold-time information.
show cdp entry	Displays information about a specific neighbor device or all neighboring devices discovered using CDP.

Command	Description
show cdp neighbors	Displays detailed information about neighboring devices discovered using CDP.
show cdp traffic	Displays traffic information from the CDP table.

show cdp neighbors

To display detailed information about neighboring devices discovered using Cisco Discovery Protocol (CDP), use the **show cdp neighbors** command in privileged EXEC mode.

show cdp neighbors [*type number*] [**detail**]

Syntax Description

type	(Optional) Type of the interface connected to the neighbors about which you want information.
number	(Optional) Number of the interface connected to the neighbors about which you want information.
detail	(Optional) Displays detailed information about a neighbor (or neighbors) including network address, enabled protocols, hold time, and software version.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.0(3)T	The output for the **detail** form of this command was expanded to include CDP Version 2 information.

Examples

The following is sample output from the **show cdp neighbors** command:

```
Router# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme     Capability  Platform  Port ID
lab-7206         Eth 0             157          R          7206VXR   Fas 0/0/0
lab-as5300-1     Eth 0             163          R          AS5300    Fas 0
lab-as5300-2     Eth 0             159          R          AS5300    Eth 0
lab-as5300-3     Eth 0             122          R          AS5300    Eth 0
lab-as5300-4     Eth 0             132          R          AS5300    Fas 0/0
lab-3621         Eth 0             140         R S         3631-telcoFas 0/0
008024 2758E0    Eth 0             132          T          CAT3000   1/2
```

Table 47 describes the significant fields shown in the display.

Table 47 show cdp neighbors Field Descriptions

Field	Definition
Device ID	The configured ID (name), MAC address, or serial number of the neighbor device.
Local Intrfce	(Local Interface) The protocol being used by the connectivity media.

Table 47 show cdp neighbors Field Descriptions (continued)

Field	Definition
Holdtme	(Holdtime) The remaining amount of time, in seconds, the current device will hold the CDP advertisement from a transmitting router before discarding it.
Capability	The capability code discovered on the device. This is the type of the device listed in the CDP Neighbors table. Possible values are: R—Router T—Transparent bridge B—Source-routing bridge S—Switch H—Host I—IGMP device r—Repeater
Platform	The product number of the device.
Port ID	The protocol and port number of the device.

The following is sample output from the **show cdp neighbors detail** command.

```
Router# show cdp neighbors detail
-------------------------
Device ID: lab-7206
Entry address(es):
   IP address: 172.19.169.83
Platform: cisco 7206VXR,  Capabilities: Router
Interface: Ethernet0,  Port ID (outgoing port): FastEthernet0/0/0
Holdtime : 123 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 5800 Software (C5800-P4-M), Version 12.1(2)
Copyright (c) 1986-2002 by Cisco Systems, Inc.

advertisement version: 2
Duplex: half

-------------------------
Device ID: lab-as5300-1
Entry address(es):
   IP address: 172.19.169.87
Platform: cisco AS5300,  Capabilities: Router
--More--
.
.
.


Gateway#show cdp neighbors f5/1 detail

Device ID: SEP000427D400ED
Entry address(es):
  IP address: 1.6.1.81
Platform: Cisco IP Phone 7940,   Capabilities: Host
```

```
Interface: FastEthernet5/1,   Port ID (outgoing port): Port 1
Holdtime : 150 sec
Version :
P00303020204

advertisement version: 2

Duplex: full

Power drawn: 6.300 Watts
```

Table 48 describes the significant fields shown in the display.

Table 48 show cdp neighbors detail Field Descriptions

Field	Definition
Device ID	The name of the neighbor device and either the MAC address or the serial number of this device.
Entry address(es)	A list of network addresses of neighbor devices.
[network protocol] address	The network address of the neighbor device. The address can be in IP, IPX, AppleTalk, DECnet, or CLNS protocol conventions.
Platform	The product name and number of the neighbor device.
Capabilities	The device type of the neighbor. This device can be a router, a bridge, a transparent bridge, a source-routing bridge, a switch, a host, an IGMP device, or a repeater.
Interface	The protocol and port number of the port on the current device.
Holdtime	The remaining amount of time, in seconds, the current device will hold the CDP advertisement from a transmitting router before discarding it.
Version:	The software version running on the neighbor device.
advertisement version:	The version of CDP being used for CDP advertisements.
Duplex:	The duplex state of connection between the current device and the neighbor device.
Native VLAN	The ID number of the VLAN on the neighbor device.
VTP Management Domain	A string that is the name of the collective group of VLANs associated with the neighbor device.
Power Drawn:	The maximum requested power. **Note** For IP Phones the value shown is the maximum requested power (6.3 Watts). This value can be different than the actual power supplied by the routing device (generally 5 watts; shown using the **show power** command).

Related Commands

Command	Description
show cdp	Displays global CDP information, including timer and hold-time information.
show cdp entry	Displays information about a specific neighbor device listed in the CDP table.
show cdp interface	Displays information about the interfaces on which CDP is enabled.
show cdp traffic	Displays information about traffic between devices gathered using CDP.

show cdp traffic

To display information about traffic between devices gathered using Cisco Discovery Protocol (CDP), use the **show cdp traffic** command in privileged EXEC mode.

show cdp traffic

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.

Examples

The following is sample output from the **show cdp traffic** command:

```
Router# show cdp traffic

Total packets output: 543, Input: 333
Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
No memory: 0, Invalid: 0, Fragmented: 0
CDP version 1 advertisements output: 191, Input: 187
CDP version 2 advertisements output: 352, Input: 146
```

Table 49 describes the significant fields shown in the display.

Table 49 show cdp traffic Field Descriptions

Field	Definition
Total packets output	The number of CDP advertisements sent by the local device. Note that this value is the sum of the CDP Version 1 advertisements output and CDP Version 2 advertisements output fields.
Input	The number of CDP advertisements received by the local device. Note that this value is the sum of the CDP Version 1 advertisements input and CDP Version 2 advertisements input fields.
Hdr syntax	The number of CDP advertisements with bad headers, received by the local device.
Chksum error	The number of times the checksum (verifying) operation failed on incoming CDP advertisements.
Encaps failed	The number of times CDP failed to send advertisements on an interface because of a failure caused by the bridge port of the local device.

Table 49 show cdp traffic Field Descriptions (continued)

Field	Definition
No memory	The number of times the local device did not have enough memory to store the CDP advertisements in the advertisement cache table when the device was attempting to assemble advertisement packets for transmission and parse them when receiving them.
Invalid	The number of invalid CDP advertisements received and sent by the local device.
Fragmented	The number of times fragments or portions of a single CDP advertisement were received by the local device instead of the complete advertisement.
CDP version 1 advertisements output	The number of CDP Version 1 advertisements sent by the local device.
Input	The number of CDP Version 1 advertisements received by the local device.
CDP version 2 advertisements output	The number of CDP Version 2 advertisements sent by the local device.
Input	The number of CDP Version 2 advertisements received by the local device.

Related Commands

Command	Description
show cdp	Displays global CDP information, including timer and hold-time information.
show cdp entry	Displays information about a specific neighbor device listed in the CDP table.
show cdp interface	Displays information about the interfaces on which CDP is enabled.
show cdp neighbors	Displays detailed information about neighboring devices discovered using CDP.

show cdp

To display global Cisco Discovery Protocol (CDP) information, including timer and hold-time information, use the **show cdp** command in privileged EXEC mode.

show cdp

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.0(3)T	The output of this command was modified to include CDP Version 2 information.

Examples

The following example shows that the current router is sending CDP advertisements every 1 minute (the default setting for the **cdp timer** global configuration command). Also shown is that the current router directs its neighbors to hold its CDP advertisements for 3 minutes (the default for the **cdp holdtime** global configuration command), and that the router is enabled to send CDP Version 2 advertisements:

```
router# show cdp

Global CDP information:
Sending CDP packets every 60 seconds
Sending a holdtime value of 180 seconds
Sending CDPv2 advertisements is enabled
```

Table 50 describes the significant fields shown in the display.

Table 50 show cdp Field Descriptions

Field	Definition
Sending CDP packets every XX seconds	The interval (in seconds) between transmissions of CDP advertisements. This field is controlled by the **cdp timer** command.
Sending a holdtime value of XX seconds	The amount of time (in seconds) the device directs the neighbor to hold a CDP advertisement before discarding it. This field is controlled by the **cdp holdtime** command.
Sending CDPv2 advertisements is XX	The state of whether CDP Version-2 type advertisements are enabled to be sent. Possible states are enabled or disabled. This field is controlled by the **cdp advertise v2** global configuration command.

Related Commands

Command	Description
cdp advertise-v2	Enables CDP Version 2 advertising functionality on a device.
cdp holdtime	Specifies the amount of time the receiving device should hold a CDP packet from your router before discarding it.
cdp timer	Specifies how often the Cisco IOS software sends CDP updates.
show cdp entry	Displays information about a specific neighbor device listed in the CDP table.
show cdp interface	Displays information about the interfaces on which CDP is enabled.
show cdp neighbors	Displays detailed information about neighboring devices discovered using CDP.
show cdp traffic	Displays information about traffic between devices gathered using CDP.

show clock

To display the time and date from the system software clock, use the **show clock** command in EXEC mode.

show clock [**detail**]

Syntax Description

detail	(Optional) Indicates the clock source (NTP, VINES, hardware clock, and so on) and the current summer-time setting (if any).

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The software clock keeps an "authoritative" flag that indicates whether the time is authoritative (believed to be accurate). If the software clock has been set by a timing source (for example, via NTP), the flag is set. If the time is not authoritative, it will be used only for display purposes. Until the clock is authoritative and the "authoritative" flag is set, the flag prevents peers from synchronizing to the software clock.

The symbol that precedes the **show clock** display indicates the following:

Symbol	Description	Example
*	Time is not authoritative: the software clock is not in sync or has never been set.	*15:29:03.158 UTC Tue Feb 25 2003:
(blank)	Time is authoritative: the software clock is in sync or has just been set manually	15:29:03.158 UTC Tue Feb 25 2003:
.	Time is authoritative, but NTP is not synchronized: the software clock was in sync, but has since lost contact with all configured NTP servers	.15:29:03.158 UTC Tue Feb 25 2003:

These symbols are also used in NTP-based timestamping, such as for syslog (SEM) messages.

Note In general, NTP synchronization takes approximately 15 to 20 minutes.

Examples

The following sample output shows that the current clock is authoritative and that the time source is NTP:

```
Router> show clock detail

15:29:03.158 PST Tue Feb 25 2003
Time source is NTP
```

The following example shows the current clock is authoritative, but NTP is not yet synchronized:

```
Router> show clock

.16:42:35.597 UTC Tue Feb 25 2003
```

Related Commands

Command	Description
clock set	Manually sets the software clock.
show calendar	Displays the current time and date setting of the system hardware clock.

show cls

To display the current status of all Cisco link services (CLS) sessions on the router, use the **show cls** command in EXEC mode.

show cls [**brief**]

Syntax Description

brief	(Optional) Displays a brief version of the output.

Defaults

Without the **brief** keyword, displays complete output.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced in a release prior to Cisco IOS Release 11.0.

Usage Guidelines

The Cisco link service (CLS) is used as the interface between data link users (DLUs), such as DLSw, LAN Network Manager (LNM), downstream physical unit (DSPU), and SNASw, and their corresponding data link circuits (DLCs) such as Logic Link Control (LLC), VDLC, and Qualified Logic Link Control (QLLC). Each DLU registers a particular service access point (SAP) with CLS, and establishes circuits through CLS over the DLC.

The **show cls** command displays the SAP values associated with the DLU and the circuits established through CLS.

For further information about CLS, use the *Cisco IOS Bridging and IBM Networking Configuration Guide*.

Examples

The following is sample output from the **show cls** command:

```
IBD-4500B# show cls

DLU user:SNASW
   SSap:0x04  VDLC VDLC650
    DTE:1234.4000.0001 1234.4000.0002 04 04
    T1 timer:0   T2 timer:0  Inact timer:0
    max out:0    max in:0    retry count:10
    XID retry:10 XID timer:5000  I-Frame:0
    flow:0       DataIndQ:0   DataReqQ:0
DLU user:DLSWDLUPEER
DLU user:DLSWDLU
   Bridging  VDLC VDLC1000
   Bridging  VDLC VDLC650
```

The following is sample output from the **show cls brief** command:

```
IBD-4500B# show cls brief
```

```
DLU user:SNASW
   SSap:0x04  VDLC VDLC650
    DTE:1234.4000.0001 1234.4000.0002 04 04
DLU user:DLSWDLUPEER
DLU user:DLSWDLU
   Bridging  VDLC VDLC1000
   Bridging  VDLC VDLC650
```

The examples show two DLUs—SNASw and DLSw—active in the router. SNASw uses a SAP value of 0x04, and the associated DLC port is VDLC650. SNASw has a circuit established between MAC addresses 1234.4000.0001 and 1234.4000.0002 using source and destination SAPs 04 and 04. DLSw is a bridging protocol and uses VDLC1000 and VDLC650 ports. There are no circuits in place at this time.

In the output from the **show cls** command (without the **brief** argument), the values of timers and counters applicable to this circuit are displayed.

Related Commands

Command	Description
stun peer-name	Enables STUN for an IP address and uses Cisco Link Services (CLS) to access the Frame Relay network.

show cns config connections

To display the status of the Cisco Networking Services (CNS) event agent connection, use the **show cns config connections** command in privileged EXEC mode.

show cns config connections

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Use the **show cns config connections** command to determine whether the CNS event agent is connecting to the gateway, connected, or active, and to display the gateway used by the event agent and its IP address and port number.

Examples

The following is sample output from the **show cns config connections** command:

```
Router# show cns config connections

The partial configuration agent is enabled.

Configuration server:  10.1.1.1
Port number:           80
Encryption:            disabled
Config id:             test1
Connection Status:     Connection not active.
```

Related Commands

Command	Description
show cns config outstanding	Displays information about incremental CNS configurations that have started but not yet completed.
show cns config stats	Displays statistics about the CNS configuration agent.

show cns config outstanding

To display information about incremental (partial) Cisco Networking Services (CNS) configurations that have started but not yet completed, use the **show cns config outstanding** command in privileged EXEC mode.

show cns config outstanding

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(8)T	This command was implemented on Cisco 2600 series and Cisco 3600 series routers.

Usage Guidelines

Use the **show cns config outstanding** command to display information about outstanding incremental (partial) configurations that have started but not yet completed, including the following:

- Queue ID (location of configuration in the config queue)
- Identifier (group ID)
- Config ID (identity of configuration within the group)

Examples

The following is sample output from the **show cns config outstanding** command:

```
Router# show cns config outstanding

The outstanding configuration information:
queue id   identifier       config-id
1          identifierREAD   config_idREAD
```

Related Commands

Command	Description
cns config cancel	Cancels an incremental two-phase synchronization configuration.
config-cli	Displays the status of the CNS event agent connection.
show cns config stats	Displays statistics about the CNS configuration agent.

show cns config stats

To display statistics about the CNS configuration agent, use the **show cns config stats** command in privileged EXEC mode.

show cns config stats

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(8)T	This command was implemented on Cisco 2600 series and Cisco 3600 series routers.
12.3(1)	Additional output fields were added.

Usage Guidelines

This command displays the following statistics on the CNS configuration agent:

- The number of configurations requests received
- The number of configurations completed
- The number of configurations failed
- The number of configurations pending
- The number of configurations cancelled
- The time stamp of the last configuration received
- The time stamp of the initial configuration received

Examples

The following is sample output from the **show cns config stats** command:

```
Router# show cns config stats

6 configuration requests received.
4 configurations completed.
1 configurations failed.
1 configurations pending.
0 configurations cancelled.
The time of last received configuration is *May 5 2003 10:42:15 UTC.
Initial Config received *May 5 2003 10:45:15 UTC.
```

Related Commands

Command	Description
clear cns config stats	Clears all the statistics about the CNS configuration agent.
show cns config outstanding	Displays information about incremental CNS configurations that have started but not yet completed.

show cns config status

To display the status of the Cisco Networking Services (CNS) Configuration Agent, use the **show cns config status** command in EXEC mode.

show cns config status

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0 (22)S.

Usage Guidelines

This command displays the status of the Configuration Agent. Use this option to display the following information about the Configuration Agent:

- Status of the Configuration Agent, for example, whether it has been configured properly.
- IP address and port number of the trusted server that the Configuration Agent is using.
- Config ID (identity of configuration within the configuration group).

Related Commands

Command	Description
cns config cancel	Cancels a CNS configuration.
cns config initial	Starts the initial CNS Configuration Agent.
cns config partial	Starts the partial CNS Configuration Agent.
cns config retrieve	Gets the configuration of a routing device using CNS.

show cns event connections

To display the status of the Cisco Networking Services (CNS) event agent connection, use the **show cns event connections** command in privileged EXEC mode.

show cns event connections

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Use the **show cns event connections** command to display the status of the event agent connection—such as whether it is connecting to the gateway, connected, or active—and to display the gateway used by the event agent and its IP address and port number.

Examples

The following example displays the IP address and port number of the primary and backup gateways:

```
Router# show cns event connections

The currently configured primary event gateway:
        hostname is 10.1.1.1.
        port number is 11011.
Event-Id is Internal test1
Keepalive setting:
        none.
Connection status:
        Connection Established.
The currently configured backup event gateway:
        none.
The currently connected event gateway:
        hostname is 10.1.1.1.
        port number is 11011.
```

Related Commands

Command	Description
show cns event stats	Displays statistics about the CNS event agent connection.
show cns event subject	Displays a list of subjects about the CNS event agent connection.

show cns event gateway

To display information about the Cisco Networking Services (CNS) Event Agent, use the **show cns event gateway** command in EXEC mode.

show cns event gateway

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0 (18)ST

Usage Guidelines

Use this command to display the following information about CNS gateways:

- Primary gateway:
  - IP address
  - Port number
- Backup gateways:
  - IP address
  - Port number
- Currently connected gateway:
  - IP address
  - Port number

Related Commands

Command	Description
cns event	Configures the CNS Event Gateway.

show cns event stats

To display statistics about the CNS event agent connection, use the **show cns event stats** command in privileged EXEC mode.

show cns event stats

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(8)T	This command was implemented on the Cisco 2600 series and the Cisco 3600 series routers.
12.3(1)	Output was changed to display statistics generated since last cleared.

Usage Guidelines

Use this command to display the following statistics for the CNS event agent:

- Number of events received
- Number of events sent
- Number of events not processed successfully
- Number of events in the queue
- Time stamp showing when statistics were last cleared (time stamp is router time)
- Number of events received since the statistics were cleared
- Time stamp of latest event received (time stamp is router time)
- Time stamp of latest event sent
- Number of applications using the Event Agent
- Number of subjects subscribed

Examples

The following example displays statistics for the CNS event agent:

```
Router# show cns event stats

0 events received.
1 events sent.
0 events not processed.
0 events in the queue.
0 events sent to other IOS applications.
Event agent stats last cleared at Apr 4 2003 00:55:25 UTC
```

```
No events received since stats cleared
The time stamp of the last received event is *Mar 30 2003 11:04:08 UTC
The time stamp of the last sent event is *Apr 11 2003 22:21:23 UTC
3 applications are using the event agent.
0 subjects subscribed.
1 subjects produced.
0 subjects replied.
```

Related Commands

Command	Description
clear cns event stats	Clears all the statistics about the CNS event agent.
cns event	Enables and configures CNS event agent services.
show cns event connections	Displays the status of the CNS event agent connection.
show cns event subject	Displays a list of subjects about the CNS event agent connection.

show cns event status

To display information about the Cisco Networking Services (CNS) Event Agent, use the **show cns event status** command in EXEC mode.

show cns event status

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0 (18)ST.

Usage Guidelines

Use this command to display the following information about the CNS Event Agent:

- Status of Event Agent:
  - Connected
  - Active
- Gateway used by the Event Agent:
  - IP address
  - Port number
- Device ID

Related Commands

Command	Description
cns event	Configures the CNS Event Gateway.

show cns event subject

To display a list of subjects about the Cisco Networking Services (CNS) event agent connection, use the **show cns event subject** command in privileged EXEC mode.

show cns event subject [*name*]

Syntax Description

name	(Optional) Displays a list of applications that are subscribing to this specific subject name.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(8)T	This command was implemented on the Cisco 2600 series and the Cisco 3600 series.

Usage Guidelines

Use the **show cns event subject** command to display a list of subjects of the event agent that are subscribed to by applications.

Examples

The following example displays the IP address and port number of the primary and backup gateways:

```
Router# show cns event subject

The list of subjects subscribed by applications.
   cisco.cns.mibaccess:request
   cisco.cns.config.load
   cisco.cns.config.reboot
   cisco.cns.exec.cmd
```

Related Commands

Command	Description
show cns event connections	Displays the status of the CNS event agent connection.
show cns event stats	Displays statistics about the CNS event agent connection.

show cns image connections

To display the status of the Cisco Networking Services (CNS) image management server HTTP connections, use the **show cns image connections** command in privileged EXEC mode.

show cns image connections

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use the **show cns image connections** command when troubleshooting HTTP connection problems with the CNS image server. The output displays the following information:

- Number of connection attempts
- Number of connections that were never connected and those that were abruptly disconnected
- Date and time of last successful connection

Examples

The following is sample output from the **show cns image connections** command:

```
Router# show cns image connections

CNS Image Agent:  HTTP connections
Connection attempts 1
never connected:0   Abrupt disconnect:0
Last successful connection at 11:45:02.000 UTC Mon May 6 2003
```

Related Commands

Command	Description
show cns image inventory	Displays inventory information about the CNS image agent.
show cns image status	Displays status information about the CNS image agent.

show cns image inventory

To provide a dump of Cisco Networking Services (CNS) image inventory information in XML format, use the **show cns image inventory** command in privileged EXEC mode.

show cns image inventory

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

To view the XML output in a better format, paste the content into a text file and use an XML viewing tool.

Examples

The following is sample output from the **show cns image inventory** command:

```
Router# show cns image inventory

Inventory Report
<imageInventoryReport><deviceName><imageID>Router</imageID><hostName>Router</ho
IOS (tm) C2600 Software (C2600-I-M), Experimental Version 12.3(20030414:081500)]
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Mon 14-Apr-03 02:03 by engineer</versionString><imageFile>tftp://10.25>
```

Related Commands

Command	Description
show cns image connections	Displays connection information for the CNS image agent.
show cns image status	Displays status information about the CNS image agent.

show cns image status

To display status information about the Cisco Networking Services (CNS) image agent, use the **show cns image status** command in privileged EXEC mode.

show cns image status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use this command to display the following status information about the CNS image agent:

- Start date and time of last upgrade
- End date and time of last upgrade
- End date and time of last successful upgrade
- End date and time of last failed upgrade
- Number of failed upgrades
- Number of successful upgrades with number of received messages and errors
- Transmit status with number of attempts, successes, and failures

Examples

The following is sample output from the **show cns image status** command:

```
Router# show cns image status

Last upgrade started at 11:45:02.000 UTC Mon May 6 2003
Last upgrade ended at 11:56:04.000 UTC Mon May 6 2003 status SUCCESS

Last successful upgrade ended at 00:00:00.000 UTC Mon May 6 2003
Last failed upgrade ended at 00:00:00.000 UTC Wed Apr 16 2003
Number of failed upgrades: 2
Number of successful upgrades: 6
 messages received: 12
 receive errors: 5
Transmit Status
  TX Attempts:4
    Successes:3         Failures 2
```

Related Commands

Command	Description
show cns image connections	Displays connection information for the CNS image agent.
show cns image inventory	Displays image inventory information in XML format.

show <command> append

To redirect and add the output of any **show** command to an existing file, use the **show** *command* **| append** command in privileged EXEC mode.

show *command* **| append** *url*

Syntax Description

command	Any Cisco IOS **show** command.
| append *url*	The addition of this syntax redirects the command output to the file location specified in the Universal Resource Locator (URL). The pipe (|) is required. The Cisco IOS File System (IFS) uses URLs to specify the location of a file system, directory, and file. Typical URL elements include: *prefix***:**[*directory*/]*filename* Prefixes can be local file locations, such as **flash:** or **disk0:**. Alternatively, you can specify network locations using the following syntax: **ftp:**[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename* **tftp:**[[//*location*]/*directory*]/*filename* The **rcp:** prefix is not supported.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(21)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

To display all URL prefixes that are supported for this command, use the **show** *command* **| append ?** command.

This command adds the **show** command output to the end of the specified file.

Examples

In the following example, output from the **show tech-support** command is redirected to an existing file on Disk 1 with the file-name of "showoutput.txt." This output is added at the end of any existing data in the file.

```
Router# show tech-support | append disk1:showoutput.txt
```

Related Commands

Command	Description
show <command> redirect	Redirects the output of any **show** command to a specified file.
show <command> tee	Copies the **show** command output to a file while displaying it on the terminal.

show <command> begin

To begin the output of any **show** command from a specified string, use the **show** *command* | **begin** command in EXEC mode.

show *command* | **begin** *regular-expression*

Syntax Description

command	Any supported **show** command.
|	A vertical bar (the "pipe" symbol) indicates that an output processing specification follows.
regular-expression	Any regular expression found in **show** command output. The show output will begin from the first instance of this string (output prior to this string will not be printed to the screen). The string is case-sensitive. Use parenthesis to indicate a literal use of spaces.
/	Specifies a search at a --More-- prompt that begins unfiltered output with the first line that contains the regular expression.
-	Specifies a filter at a --More-- prompt that only displays output lines that do not contain the regular expression.
+	Specifies a filter at a --More-- prompt that only displays output lines that contain the regular expression.

Command Modes

EXEC

Command History

Release	Modification
8.3	The **show** command was introduced.
12.0(1)T	This extension of the **show** command was introduced.

Usage Guidelines

The *regular-expression* argument is case sensitive and allows for complex matching requirements. Use parenthesis to indicate a literal use of spaces. For example, **| begin u** indicates that the show output should begin with any line that contains a u; **| begin (u)** indicates that the show output should begin with any line that contains a space and a u together (line has a word that begins with a lowercase u).

To search the remaining output of the **show** command, use the following command at the --More-- prompt:

/regular-expression

You can specify a filtered search at any --More-- prompt. To filter the remaining output of the **show** command, use one of the following commands at the --More-- prompt:

-regular-expression

+regular-expression

When output volume is large, the search can produce long lists of output. To interrupt the output, press **Ctrl**-^ (Ctrl-Shift-6) or **Ctrl**-**z**.

Note Once you specify a filter for a **show** command, you cannot specify another filter at the next --More-- prompt. The first specified filter remains until the **more** command output finishes or until you interrupt the output. The use of the keyword **begin** does not constitute a filter.

Because prior output is not saved, you cannot search or filter backward through prior output.

Note A few **show** commands that have long output requirements do not require user input at the --More-- prompt to jump to the next table of output; these types of output require you to enter the same number of Ctrl-^ or Ctrl-Z combinations as there are --More-- prompts to completely abort output.

Examples

The following is partial sample output of the **show interface | begin** command that begins unfiltered output with the first line that contains the regular expression "Ethernet." At the --More-- prompt, the user specifies a filter to show only the lines in the remaining output that contain the regular expression "Serial."

```
Router# show interface | begin Ethernet
Ethernet0 is up, line protocol is up
Hardware is Lance, address is 0060.837c.6399 (bia 0060.837c.6399)
  Description: ip address is 172.1.2.14 255.255.255.0
  Internet address is 172.1.2.14/24
.
.
.
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
--More--
+Serial
filtering...
Serial1 is up, line protocol is up
Serial2 is up, line protocol is up
Serial3 is up, line protocol is down
Serial4 is down, line protocol is down
Serial5 is up, line protocol is up
Serial6 is up, line protocol is up
Serial7 is up, line protocol is up
```

Related Commands

Command	Description
more <url> begin	Begins unfiltered output of the **more** command with the first line that contains the regular expression you specify.
more <url> exclude	Filters **more** command output so that it excludes lines that contain a particular regular expression.
more <url> include	Filters **more** command output so that it displays only lines that contain a particular regular expression.
show <command> exclude	Filters **show** command output so that it excludes lines that contain a particular regular expression.
show <command> include	Filters **show** command output so that it displays only lines that contain a particular regular expression.

show <command> exclude

To filter **show** command output so that it excludes lines that contain a particular regular expression, use the **show** *command* **| exclude** command in EXEC mode.

show *command* **| exclude** *regular-expression*

Syntax Description

command	Any supported **show** command.
|	A vertical bar (the "pipe" symbol) indicates that an output processing specification follows.
regular-expression	Any regular expression found in **show** command output.
/	Specifies a search at a --More-- prompt that begins unfiltered output with the first line that contains the regular expression.

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.

Usage Guidelines

The *regular-expression* argument is case sensitive and allows for complex matching requirements.

You can specify a new search at every --More-- prompt. To search the remaining output of the **show** command, use the following syntax at the --More-- prompt:

/regular-expression

When output volume is large, the search can produce long lists of output. To interrupt the output, press **Ctrl**-^ (Ctrl-Shift-6) or **Ctrl**-**Z**.

Because prior output is not saved, you cannot search or filter backward through prior output.

Note A few **show** commands that have long output requirements do not require user input at the --More-- prompt to jump to the next table of output; these types of output require you to enter the same number of Ctrl-^ or Ctrl-Z combinations as there are --More-- prompts to completely abort output.

Examples

The following is partial sample output of the **show | exclude** command used with the **show buffers** command. It excludes lines that contain the regular expression "0 misses." At the --More-- prompt, the user searches for the regular expression "Serial0," which continues the filtered output with the first line that contains "Serial0."

```
Router# show buffers | exclude 0 misses

Buffer elements:
     398 in free list (500 max allowed)
Public buffer pools:
Small buffers, 104 bytes (total 50, permanent 50):
```

```
     50 in free list (20 min, 150 max allowed)
     551 hits, 3 misses, 0 trims, 0 created
Big buffers, 1524 bytes (total 50, permanent 50):
     49 in free list (5 min, 150 max allowed)
Very Big buffers, 4520 bytes (total 10, permanent 10):
.
.
.
Huge buffers, 18024 bytes (total 0 permanent 0):
     0 in free list (0 min, 4 max allowed)
--More--
/Serial0
filtering...
Serial0 buffers, 1543 bytes (total 64, permanent 64):
     16 in free list (0 min, 64 max allowed)
     48 hits, 0 fallbacks
```

Related Commands

Command	Description
more <url> begin	Begins unfiltered output of the **more** command with the first line that contains the regular expression you specify.
more <url> exclude	Filters **more** command output so that it excludes lines that contain a particular regular expression.
more <url> include	Filters **more** command output so that it displays only lines that contain a particular regular expression.
show <command> begin	Searches the output of any **show** command and displays the output from the first instance of a specified string.
show <command> include	Filters **show** command output so that it displays only lines that contain a particular regular expression.

show <command> include

To filter **show** command output so that it only displays lines that contain a particular regular expression, use the **show** *command* **| include** command in EXEC mode.

show *command* **| include** *regular-expression*

Syntax Description

command	Any supported **show** command.
|	A vertical bar (the "pipe" symbol) indicates that an output processing specification follows.
regular-expression	Any regular expression found in **show** command output. Use parenthesis to include spaces in the expression.
/	Specifies a search at a --More-- prompt that begins unfiltered output with the first line that contains the regular expression.

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.

Usage Guidelines

The *regular-expression* argument is case sensitive and allows for complex matching requirements.

You can specify a new search at every --More-- prompt. To search the remaining output of the **show** command, use the following syntax at the --More-- prompt:

/regular-expression

When output volume is large, the search can produce long lists of output. To interrupt the output, press **Ctrl**-^ (Ctrl-Shift-6) or **Ctrl**-**Z**.

Because prior output is not saved, you cannot search or filter backward through prior output.

Note A few **show** commands that have long output requirements do not require user input at the --More-- prompt to jump to the next table of output; these types of output require you to enter the same number of Ctrl-^ or Ctrl-Z combinations as there are --More-- prompts to completely abort output.

Examples

The following is partial sample output of the **show interface | include** command. It displays only lines that contain the regular expression "(is)." The parentheses force the inclusion of the spaces before and after "is." Use of the parenthesis ensures that only lines containing "is" with a space both before and after it will be included in the output. Lines with words like "disconnect" will be excluded because there are not spaces around the instance of the string "is".

```
Router# show interface | include ( is )

ATM0 is administratively down, line protocol is down
  Hardware is ATMizer BX-50
```

```
Dialer1 is up (spoofing), line protocol is up (spoofing)
  Hardware is Unknown
  DTR is pulsed for 1 seconds on reset
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 0060.837c.6399 (bia 0060.837c.6399)
  Internet address is 172.21.53.199/24
Ethernet1 is up, line protocol is up
  Hardware is Lance, address is 0060.837c.639c (bia 0060.837c.639c)
  Internet address is 5.5.5.99/24
Serial0:0 is down, line protocol is down
  Hardware is DSX1
.
.
.
 --More--
```

At the --More-- prompt, the user searches for the regular expression “Serial0:13”, which continues filtered output with the first line that contains “Serial0:13.”

```
/Serial0:13
filtering...
Serial0:13 is down, line protocol is down
  Hardware is DSX1
  Internet address is 11.0.0.2/8
     0 output errors, 0 collisions, 2 interface resets
  Timeslot(s) Used:14, Transmitter delay is 0 flags
```

Related Commands

Command	Description
more <url> begin	Begins unfiltered output of the **more** command with the first line that contains the regular expression you specify.
more <url> exclude	Filters **more** command output so that it excludes lines that contain a particular regular expression.
more <url> include	Filters **more** command output so that it displays only lines that contain a particular regular expression.
show <command> begin	Searches the output of any **show** command and displays the output from the first instance of a specified string.
show <command> exclude	Filters **show** command output so that it excludes lines that contain a particular regular expression.

show <command> redirect

To redirect the output of any **show** command to a file, use the **show** *command* **| redirect** command in privileged EXEC mode.

show *command* **| redirect** *url*

Syntax Description

command	Any Cisco IOS **show** command.
| redirect *url*	The addition of this syntax redirects the command output to the file location specified in the Universal Resource Locator (URL). The pipe (|) is required. The Cisco IOS File System (IFS) uses URLs to specify the location of a file system, directory, and file. Typical URL elements include: *prefix***:**[*directory*/]*filename* Prefixes can be local file locations, such as **flash:** or **disk0:**. Alternatively, you can specify network locations using the following syntax: **ftp:**[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename* **tftp:**[[//*location*]/*directory*]/*filename* The **rcp:** prefix is not supported.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(21)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

To display all URL prefixes that are supported for this command, use the **show** *command* **| redirect ?** command.

This command creates a new file at the specified location, or overwrites an existing file.

Examples

In the following example, output from the **show tech-support** command is write to the file "showtech.txt" on the host at 172.16.101.101 in the directory "//tftpboot/docs/" using FTP:

```
Router# show tech | redirect
ftp://USER:MYPASSWORD@172.16.101.101//tftpboot/docs/showtech.txt
```

Related Commands

Command	Description
show <command> append	Redirects and appends **show** command output to the end of an existing file.
show <command> tee	Copies the **show** command output to a file while displaying it on the terminal.

show <command> tee

To copy the output of any **show** command to a file while displaying it on the terminal, use the **show** *command* **|** **tee** command in privileged EXEC mode.

show *command* **|** **tee** [/**append**] *url*

Syntax Description

command	Any Cisco IOS **show** command.
| tee *url*	The addition of this syntax copies the command output to the file location specified in the Universal Resource Locator (URL). The pipe (|) is required. The Cisco IOS File System (IFS) uses URLs to specify the location of a file system, directory, and file. Typical URL elements include: *prefix***:**[*directory*/]*filename* Prefixes can be local file locations, such as **flash:** or **disk0:**. Alternatively, you can specify network locations using the following syntax: **ftp:**[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename* **tftp:**[[//*location*]/*directory*]/*filename* The **rcp:** prefix is not supported.
/append	(Optional) Adds the **show** command output to the end of an existing file.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(21)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

To display all URL prefixes that are supported for this command, use the **show** *command* **|** **tee ?** command.

The **tee** keyword was chosen to reflect that output is redirected to two locations; the terminal and a file (as a tee plumbing junction redirects water to two different pipes).

Examples

In the following example, output from the **show tech-support** command is displayed on-screen while it is written to the file "showoutput.txt" at the host 172.16.101.101 using TFTP:

```
Router# show tech-support | tee tftp://172.16.101.101/docs/showoutput.txt
```

The following example performs the same function as above, but in this case the output is added at the end of any existing data in the file "showoutput.txt":

```
Router# show tech-support | tee /append tftp://172.16.101.101/docs/showoutput.txt
```

Related Commands

Command	Description
show <command> append	Redirects the output of any **show** command and adds it to the end of existing file.
show <command> redirect	Redirects the output of any **show** command to a specified file.

show context

To display information stored in NVRAM when an unexpected system reload (system exception) occurs, use the **show context** command in user EXEC or priviledged EXEC mode.

show context [**summary** | **all** | **slot** *slot-number* [*crash-index*] [**all**] [**debug**]]

Syntax Description

summary	Displays a summary of all the crashes recorded.
all	Displays all crashes for all the slots. When optionally used with the **slot** keyword, displays crash information for the specified slot.
slot *slot-number* [*crash-index*]	Displays information for a particular line card. Slot numbers range from 0 to 11 for the Cisco 12012 router and from 0 to 7 for the Cisco 12008. The index number allows you to look at previous crash contexts. Contexts from the last 24 line card crashes are saved on the GRP card. If the GRP reloads, the last 24 line card crash contexts are lost. For example, **show context slot 3 2** shows the second most recent crash for line card in slot 3. Index numbers are displayed by the **show context summary** command.
debug	(Optional) Displays crash information as a hex record dump in addition to one of the options listed.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
11.2 GS	The **slot** *slot-number* [*crash-index*] [**all**] [**debug**] syntax was added for Cisco 12000 series routers.

Usage Guidelines

The display from the **show context** command includes the following information:

- Reason for the system reboot
- Stack trace
- Software version
- The signal number, code, and router uptime information
- All the register contents at the time of the crash

Note This command is primarily for use by Cisco technical support representatives for analyzing unexpected system reloads.

Output for this command will vary by platform. Context information is specific to processors and architectures. For example, context information for the Cisco 2600 series router differs from that for other router types because the Cisco 2600 runs with an M860 processor.

Examples

The following is sample output from the **show context** command following a system failure:

```
Router> show context

System was restarted by error - a Software forced crash, PC 0x60189354
GS Software (RSP-PV-M), Experimental Version 11.1(2033) [ganesh 111]
Compiled Mon 31-Mar-97 13:21 by ganesh
Image text-base: 0x60010900, data-base: 0x6073E000
Stack trace from system failure:
FP: 0x60AEA798, RA: 0x60189354
FP: 0x60AEA798, RA: 0x601853CC
FP: 0x60AEA7C0, RA: 0x6015E98C
FP: 0x60AEA7F8, RA: 0x6011AB3C
FP: 0x60AEA828, RA: 0x601706CC
FP: 0x60AEA878, RA: 0x60116340
FP: 0x60AEA890, RA: 0x6011632C
Fault History Buffer:
GS Software (RSP-PV-M), Experimental Version 11.1(2033) [ganesh 111]
Compiled Mon 31-Mar-97 13:21 by ganesh
Signal = 23, Code = 0x24, Uptime 00:04:19
$0 : 00000000, AT : 60930120, v0 : 00000032, v1 : 00000120
a0 : 60170110, a1 : 6097F22C, a2 : 00000000, a3 : 00000000
t0 : 60AE02A0, t1 : 8000FD80, t2 : 34008F00, t3 : FFFF00FF
t4 : 00000083, t5 : 3E840024, t6 : 00000000, t7 : 11010132
s0 : 00000006, s1 : 607A25F8, s2 : 00000001, s3 : 00000000
s4 : 00000000, s5 : 00000000, s6 : 00000000, s7 : 6097F755
t8 : 600FABBC, t9 : 00000000, k0 : 30408401, k1 : 30410000
gp : 608B9860, sp : 60AEA798, s8 : 00000000, ra : 601853CC
EPC : 60189354, SREG : 3400EF03, Cause : 00000024
Router>
```

The following is sample output from the **show context summary** command on a Cisco 12012 router. The **show context summary** command displays a summary of all the crashes recorded for each slot (line card).

```
Router# show context summary

CRASH INFO SUMMARY
  Slot 0 : 0 crashes
  Slot 1 : 0 crashes
  Slot 2 : 0 crashes
  Slot 3 : 0 crashes
  Slot 4 : 0 crashes
  Slot 5 : 0 crashes
  Slot 6 : 0 crashes
  Slot 7 : 2 crashes
    1 - crash at 18:06:41 UTC Tue Nov 5 1996
    2 - crash at 12:14:55 UTC Mon Nov 4 1996
  Slot 8 : 0 crashes
  Slot 9 : 0 crashes
  Slot 10: 0 crashes
  Slot 11: 0 crashes
Router#
```

The following is sample output from the **show context** command following an unexpected system reload on a Cisco 2600 series router.

```
router# show context

S/W Version: Cisco IOS Software
Cisco IOS (tm) c2600 Software (c2600-JS-M), Released Version 11.3(19980115:184921]
Copyright (c) 1986-2003 by Cisco Systems, Inc.
Compiled Thu 15-Jan-98 13:49 by mmagno
Exception occurred at: 00:02:26 UTC Mon Mar 1 1993
```

```
Exception type: Data TLB Miss (0x1200)
CPU Register Context:
PC   = 0x80109964  MSR = 0x00009030  CR  = 0x55FFFD35  LR    = 0x80109958
CTR = 0x800154E4  XER = 0xC000BB6F  DAR = 0x00000088  DSISR = 0x00000249
DEC = 0x7FFFDFCA  TBU = 0x00000000  TBL = 0x15433FCF  IMMR  = 0x68010020
R0   = 0x80000000  R1  = 0x80E80BD0  R2  = 0x80000000  R3    = 0x00000000
R4   = 0x80E80BC0  R5  = 0x40800000  R6  = 0x00000001  R7    = 0x68010000
R8   = 0x00000000  R9  = 0x00000060  R10 = 0x00001030  R11   = 0xFFFFFFFF
R12 = 0x00007CE6  R13 = 0xFFF379E8  R14 = 0x80D50000  R15   = 0x00000000
R16 = 0x00000000  R17 = 0x00000000  R18 = 0x00000000  R19   = 0x00000000
R20 = 0x00000000  R21 = 0x00000001  R22 = 0x00000010  R23   = 0x00000000
R24 = 0x00000000  R25 = 0x80E91348  R26 = 0x01936010  R27   = 0x80E92A80
R28 = 0x00000001  R29 = 0x019BA920  R30 = 0x00000000  R31   = 0x00000018
Stack trace:
Frame 00: SP = 0x80E80BD0    PC = 0x80109958
Frame 01: SP = 0x80E80C28    PC = 0x8010A720
Frame 02: SP = 0x80E80C40    PC = 0x80271010
Frame 03: SP = 0x80E80C50    PC = 0x8025EE64
Frame 04: SP = 0x80DEE548    PC = 0x8026702C
Frame 05: SP = 0x80DEE558    PC = 0x8026702C
```

Table 51 describes the significant fields shown in the display.

Table 51 show context Field Descriptions

Field	Description
S/W Version	Standard Cisco IOS version string as displayed.
Exception occurred at	Router real time when exception occurred. The router must have the clock time properly configured for this to be accurate.
Exception type	Technical reason for exception. For engineering analysis.
CPU Register Context	Technical processor state information. For engineering analysis.
Stack trace	Technical processor state information. For engineering analysis.

Related Commands

Command	Description
show processes	Displays information about the active processes.
show stacks	Monitors the stack usage of processes and interrupt routines.

show controllers (GRP image)

To display information that is specific to the hardware, use the **show controllers** command in privileged EXEC mode.

show controllers [**atm** *slot-number* | **clock** | **csar** [**register**] | **csc-fpga** | **dp83800** | **fab-clk** | **fia** [**register**] | **pos** [*slot-number*] [**details**] | **queues** [*slot-number*] | **sca** | **xbar**]

Syntax Description

atm *slot-number*	(Optional) Displays the ATM controllers. Number is slot-number/port-number (for example, 4/0). Slot numbers range from 0 to 11 for the Cisco 12012 router and from 0 to 7 for the Cisco 12008 router.
clock	(Optional) Displays the clock card configuration.
csar [**register**]	(Optional) Displays the Cisco Cell Segmentation and Reassembly (CSAR) information. CSAR is the name of the chip on the card that handles traffic between the GRP and the switch fabric interface ASICs.
csc-fpga	(Optional) Displays the clock and scheduler card register information in the field programmable gate array (FPGA).
dp83800	(Optional) Displays the Ethernet information on the GRP card.
fab-clk	(Optional) Display the switch fabric clock register information. The switch fabric clock FPGA is a chip that monitors the incoming fabric clock generated by the switch fabric. This clock is needed by each card connecting to the switch fabric to properly communicate with it. Two switch fabric clocks arrive at each card; only one can be used. The FPGA monitors both clocks and selects which one to use if only one of them is running.
fia [**register**]	(Optional) Displays the fabric interface ASIC information and optionally displays the register information.
pos [slot-*number*] [**details**]	(Optional) Displays the POS framer state and optionally displays all the details for the interface. Number is slot-number/port-number (for example, 4/0). Slot numbers range from 0 to 11 for the Cisco 12012 router and from 0 to 7 for the Cisco 12008 router.
queues [*slot-number*]	(Optional) Displays the SDRAM buffer carve information and optionally displays the information for a specific line card. The SDRAM buffer carve information displayed is suggested carve information from the GRP card to the line card. Line cards might change the shown percentages based on SDRAM available. Slot numbers range from 0 to 11 for the Cisco 12012 router and from 0 to 7 for the Cisco 12008.
sca	(Optional) Displays the SCA register information. The SCA is an ASIC that arbitrates among the line cards requests to use the switch fabric.
xbar	(Optional) Displays the crossbar register information. The XBAR is an ASIC that switches the data as it passes through the switch fabric.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2 GS	This command was introduced to support the Cisco 12000 series routers.

Usage Guidelines

This information provided by this command is intended for use only by technical support representatives in analyzing system failures in the field.

Examples

The following is sample output from the **show controllers pos** command for a Cisco 12012:

```
Router# show controllers pos 7/0

POS7/0
SECTION
  LOF = 2          LOS = 0                          BIP(B1) = 5889
  Active Alarms: None
LINE
  AIS = 2          RDI = 2          FEBE = 146      BIP(B2) = 2106453
  Active Alarms: None
PATH
  AIS = 2          RDI = 4          FEBE = 63       BIP(B3) = 3216
  LOP = 0          PSE = 8          NSE = 3         NEWPTR = 2
  Active Alarms: None
APS
  COAPS = 3          PSBF = 2
  State: PSBF_state = False
  Rx(K1/K2): F0/15  Tx(K1/K2): 00/00
  S1S0 = 00, C2 = 64
PATH TRACE BUFFER : STABLE
  Remote hostname : GSR-C
  Remote interface: POS10/0
  Remote IP addr  : 10.201.101.2
  Remote Rx(K1/K2): F0/15  Tx(K1/K2): 00/00
Router#
```

Related Commands

Command	Description
clear controllers	Resets the T1 or E1 controller.
show controllers (line card image)	Displays information that is specific to the hardware on a line card.

show controllers (line card image)

To display information that is specific to the hardware on a line card, use the **attach** command in privileged EXEC mode to connect to the line card and then use the **show controllers** command in privileged EXEC mode or the **execute-on** command in privileged EXEC mode.

show controllers atm [[*port-number*] [**all** | **sar** | **summary**]]

show controllers fia [**register**]

show controllers {**frfab** | **tofab**} {**bma** {**microcode** | **ms-inst** | **register**} | **qelem** *start-queue-element* [*end-queue-element*] | **qnum** *start-queue-number* [*end-queue-number*] | **queues** | **statistics**}

show controllers io

show controllers l3

show controllers pos {**framers** | **queues** | **registers** | **rxsram** *port-number queue-start-address* [*queue-length*] | **txsram** *port-number queue-start-address* [*queue-length*]}

Syntax Description

atm	Displays the ATM controller information.
port-number	(Optional) Displays request for the physical interface on the ATM card. The range of choices is from 0 to 3.
all	(Optional) Lists all details.
sar	(Optional) Lists SAR interactive command.
summary	(Optional) Lists SAR status summary.
fia	Displays the fabric interface ASIC information.
register	(Optional) Displays the register information.
frfab	(Optional) Displays the "from" (transmit) fabric information.
tofab	(Optional) Displays the "to" (receive) fabric information.
bma	For the **frfab** or **tofab** keywords, displays microcode, micro sequencer, or register information for the silicon queuing engine (SQE), also known as the buffer management ASIC (BMA).
microcode	Displays SQE information for the microcode bundled in the line card and currently running version.
mis-inst	Displays SQE information for the micro sequencer instruction.
register	Displays silicon queuing engine (SQE) information for the register.
qelem	For the **frfab** or **tofab** keywords, displays the SDRAM buffer pool queue element summary information.
start-queue-element	Specifies the start queue element number from 0 to 65535.
end-queue-element	(Optional) Specifies the end queue element number from 0 to 65535).
qnum	For the **frfab** or **tofab** keywords, displays the SDRAM buffer pool queue detail information.

start-queue-number	Specifies the start free queue number (from 0 to 127).
end-queue-number	(Optional) Specifies the end free queue number (from 0 to 127).
queues	For the **frfab** or **tofab** keywords, displays the SDRAM buffer pool information.
statistics	For the **frfab** or **tofab** keywords, displays the BMA counters.
io	Displays input/output registers.
l3	Displays Layer 3 ASIC information.
pos	Displays packet-over-sonic (POS) information for framer registers, framer queues, and ASIC registers.
framers	Displays the POS framer registers.
queues	Displays the POS framer queue information.
registers	Displays the ASIC registers.
rxsram	Displays the receive queue SRAM.
port-number	Specifies a port number (valid range is from 0 to 3).
queue-start-address	Specifies the queue SRAM logical starting address.
queue-length	(Optional) Specifies the queue SRAM length.
txsram	Displays the transmit queue SRAM.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2 GS	This command was added to support the Cisco 12000 series Gigabit Switch Routers.

Usage Guidelines

This information displayed by this command is of use only to technical support representatives in analyzing unexpected system failures in the field. It is documented here in case you need to provide the displayed statistics to an technical support engineer.

Examples

Because you are executing this command on the line card, you must use the **execute-on** command to use the **show** command, or you must connect to the card using the **attach** command. All examples in this section use the **execute-on** command

The following is partial sample output from the **show controllers atm** command:

```
Router# execute-on slot 4 show controllers atm 0

TX SAR (Beta 1.0.0) is Operational;
RX SAR (Beta 1.0.0) is Operational;

Interface Configuration Mode:
        STS-12c

Active Maker Channels: total # 6
VCID  ChnnlID  Type  OutputInfo    InPkts   InOAMs  MacString
```

```
  1   0888    UBR    0C010010          0         0  08882000AAAA030000000800
  2   0988    VBR    04010020          0         0  09882000
  3   8BC8    UBR    0C010030          0         0  8BC82000AAAA030000000800
  4   0E08    UBR    0C010040          0         0  0E082000AAAA030000000800
 10   1288    VBR    040100A0          0         0  12882000
 11   8BE8    VBR    0C0100B0          0         0  8BE82000AAAA030000000800

SAR Total Counters:
total_tx_idle_cells 215267  total_tx_paks 0  total_tx_abort_paks 0
total_rx_paks 0  total_rx_drop_paks 0  total_rx_discard_cells 15

Switching Code Counters:
total_rx_crc_err_paks 0  total_rx_giant_paks 0
total_rx_abort_paks 0  total_rx_crc10_cells 0
total_rx_tmout_paks 0  total_rx_unknown_paks 0
total_rx_out_buf_paks 0  total_rx_unknown_vc_paks 0
BATMAN Asic Register Values:
hi_addr_reg 0x8000, lo_addr_reg 0x000C, boot_msk_addr 0x0780,
rmcell_msk_addr 0x0724, rmcnt__msk_addr 0x07C2, txbuf_msk_addr 0x070C,
.
.
.
CM622 SAR Boot Configuration:
txind_q_addr 0x14000 txcmd_q_addr 0x20000
.
.
.
SUNI-622 Framer Register Values:
Master Rst and Ident/Load Meters Reg (#0x0): 0x10
Master Configuration Reg (#0x1): 0x1F
Master Interrupt Status Reg (#0x2): 0x00
PISO Interrupt Reg (#0x3): 0x04
Master Auto Alarm Reg (#0x4): 0x03
Master Auto Alarm Reg (#0x5): 0x07
Parallel Output Port Reg (#0x6): 0x02
.
.
.
BERM Line BIP Threshold LSB Reg (#0x74): 0x00
BERM Line BIP Threshold MSB Reg (#0x75): 0x00
Router#
```

The following is partial sample output from the **show controllers** command:

```
Router# execute-on slot 6 show controllers

Interface POS0
Hardware is BFLC POS
lcpos_instance struct   60311B40
RX POS ASIC addr space  12000000
TX POS ASIC addr space  12000100
SUNI framer addr space  12000400
SUNI rsop intr status   00
CRC32 enabled, HDLC enc, int clock
no loop

Interface POS1
Hardware is BFLC POS
lcpos_instance struct   603142E0
RX POS ASIC addr space  12000000
TX POS ASIC addr space  12000100
SUNI framer addr space  12000600
SUNI rsop intr status   00
CRC32 enabled, HDLC enc, int clock
```

```
no loop
.
.
.
Router#
```

The following is partial sample output from the **show controllers pos framers** command:

```
Router# execute-on slot 6 show controllers pos framers

Framer 0, addr=0x12000400:
master reset            C0
master config           1F        rrate sts3c trate sts3c fixptr
master control          00
clock rcv cntrl         D0
RACP control            84
RACP gfc control        0F
TACP control status     04        hcsadd
RACP intr enable        04
RSOP cntrl intr enable  00
RSOP intr status        00
TPOP path sig lbl (c2)  13
SPTB control            04        tnull
SPTB status             00

Framer 1, addr=0x12000600:
master reset            C0
master config           1F        rrate sts3c trate sts3c fixptr
master control          00
clock rcv cntrl         D0
RACP control            84
RACP gfc control        0F
TACP control status     04        hcsadd
RACP intr enable        04
RSOP cntrl intr enable  00
RSOP intr status        00
TPOP path sig lbl (c2)  13
SPTB control            04        tnull
SPTB status             00

Framer 2, addr=0x12000800:
master reset            C0
master config           1F        rrate sts3c trate sts3c fixptr
master control          00
clock rcv cntrl         D0
RACP control            84
RACP gfc control        0F
TACP control status     04        hcsadd
RACP intr enable        04
RSOP cntrl intr enable  00
RSOP intr status        00
TPOP path sig lbl (c2)  13
SPTB control            04        tnull
SPTB status             00
.
.
.
Router#
```

The following is partial sample output from the **show controllers fia** command:

```
Router# execute-on slot 7 show controllers fia

========= Line Card (Slot 7) =======

Fabric configuration: Full bandwidth redundant
Master Scheduler: Slot 17

From Fabric FIA Errors
----------------------
redund fifo parity 0          redund overflow 0          cell drops 0
crc32 lkup parity  0          cell parity     0          crc32      0
          0          1          2          3          4
       --------   --------   --------   --------   --------
los    0          0          0          0          0
crc16  0          0          0          0          0

To Fabric FIA Errors
----------------------
sca not pres 0          req error     0          uni fifo overflow 0
grant parity 0          multi req     0          uni fifo undrflow 0
cntrl parity 0          uni req       0          crc32 lkup parity 0
multi fifo   0          empty dst req 0          handshake error   0
```

Related Commands

Command	Description
clear controllers	Resets the T1 or E1 controller.

show controllers logging

To display logging information about a Versatile Interface Processor (VIP) card, use the **show controllers logging** command in privileged EXEC mode.

show controllers vip *slot-number* **logging**

Syntax Description

vip *slot-number*	VIP slot number.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command displays the state of syslog error and event logging, including host addresses, and whether console logging is enabled.

Examples

The following is sample output from the **show controllers logging** command:

```
Router# show controllers vip 4 logging

Syslog logging: enabled
     Console logging: disabled
     Monitor logging: level debugging, 266 messages logged.
     Trap logging: level informational, 266 messages logged.
     Logging to 192.180.2.238
```

Table 52 describes the significant fields shown in the display.

Table 52 show controllers logging Field Descriptions

Field	Description
Syslog logging	When enabled, system logging messages are sent to a UNIX host that acts as a syslog server; that is, it captures and saves the messages.
Console logging	If enabled, states the level; otherwise, this field displays disabled.
Monitor logging	Minimum level of severity required for a log message to be sent to a monitor terminal (not the console).
Trap logging	Minimum level of severity required for a log message to be sent to a syslog server.

Related Commands

Command	Description
show logging	Displays the state of logging (syslog).

show controllers tech-support

To display general information about a Versatile Interface Processor (VIP) card when reporting a problem, use the **show controllers tech-support** command in privileged EXEC mode.

show controllers vip *slot-number* **tech-support**

Syntax Description

vip *slot-number*	VIP slot number.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to help collect general information about a VIP card when you are reporting a problem. This command displays the equivalent of the following **show** commands for the VIP card:

- **more system:running-config**
- **show buffers**
- **show controllers**
- **show interfaces**
- **show processes cpu**
- **show processes memory**
- **show stacks**
- **show version**

For a sample display of the **show controllers tech-support** command output, refer to these **show** commands.

Related Commands

Command	Description
more system:running-config	Displays the running configuration.
show buffers	Displays statistics for the buffer pools on the network server.
show controllers	Displays information that is specific to the hardware.
show interfaces	Uses the **show interfaces** EXEC command to display ALC information.
show processes	Displays information about the active processes.
show processes memory	Displays memory used.
show stacks	Monitors the stack usage of processes and interrupt routines.

Command	Description
show tech-support	Displays general information about the router when reporting a problem.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

show debugging

To display information about the types of debugging that are enabled for your router, use the **show debugging** command in privileged EXEC mode.

show debugging

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1	This command was introduced.

Examples

The following is sample output from the **show debugging** command. In this example, three types of CDP debugging are enabled.

```
Router# show debugging

CDP:
  CDP packet info debugging is on
  CDP events debugging is on
  CDP neighbor info debugging is on
```

Related Commands

Command	Description
debug	Begin message logging for the specified **debug** command

show derived-config

To display the composite results of all the configuration commands that apply to an interface, including commands that come from sources such as static templates, dynamic templates, dialer interfaces, and authentication, authorization, and accounting (AAA) per-user attributes, use the **show derived-config** command in privileged EXEC mode.

show derived-config [interface *type number*]

Syntax Description

interface *type number*	(Optional) Displays the derived configuration for a specific interface. If you use the **interface** keyword, you must specify the interface type and the interface number (for example, interface ethernet 0).

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

Configuration commands can be applied to an interface from sources such as static templates, dynamic templates bound by resource pooling, dialer interfaces, AAA per-user attributes and the configuration of the physical interface. The **show derived-config** command displays all the commands that apply to an interface.

The output for the **show derived-config** command is nearly identical to that of the **show running-config** command. It differs when the configuration for an interface is derived from a template, a dialer interface, or some per-user configuration. In those cases, the commands derived from the template, dialer interface, and so on, will be displayed for the affected interface.

If the same command is configured differently in two different sources that apply to the same interface, the command coming from the source that has the highest precedence will appear in the display.

Examples

The following examples show sample output for the **show running-config** and **show derived-config** commands for serial interface 0:23 and dialer interface 0. The output of the **show running-config** and **show derived-config** commands is the same for dialer interface 0 because none of the commands that apply to that interface are derived from any sources other than the configuration of the dialer interface. The output for the **show running-config** and **show derived-config** commands for serial interface 0:23 differs because some of the commands that apply to serial interface 0:23 come from dialer interface 0.

```
Router# show running-config interface Serial0:23

Building configuration...

Current configuration :296 bytes
!
interface Serial0:23
 description PRI to ADTRAN (#4444150)
 ip unnumbered Loopback0
 encapsulation ppp
```

```
 dialer rotary-group 0
 isdn switch-type primary-dms100
 isdn incoming-voice modem
 isdn calling-number 4444150
 peer default ip address pool old_pool
end

Router# show running-config interface Dialer0

Building configuration...

Current configuration :257 bytes
!
interface Dialer0
 description Dialin Users
 ip unnumbered Loopback0
 no ip proxy-arp
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 30
 dialer-group 1
 peer default ip address pool new_pool
 ppp authentication pap chap callin
end

Router# show derived-config interface Serial0:23

Building configuration...

Derived configuration :332 bytes
!
interface Serial0:23
 description PRI to ADTRAN (#4444150)
 ip unnumbered Loopback0
 encapsulation ppp
 dialer rotary-group 0
 isdn switch-type primary-dms100
 isdn incoming-voice modem
 isdn calling-number 4444150
 peer default ip address pool new_pool
 ppp authentication pap chap callin
end

Router# show derived-config interface Dialer0

Building configuration...

Derived configuration :257 bytes
!
interface Dialer0
 description Dialin Users
 ip unnumbered Loopback0
 no ip proxy-arp
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 30
 dialer-group 1
 peer default ip address pool new_pool
 ppp authentication pap chap callin
end
```

Related Commands

Command	Description
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface.

show disk

To display flash or file system information for a disk, use the **show disk** command in user EXEC or privileged EXEC mode.

show {**disk0** | **disk1**} [**all** | **filesys**]

Syntax Description

disk0	Selects disk 0 as the disk for which to display information.
disk1	Selects disk 1 as the disk for which to display information.
all	(Optional) Specifies that all flash information be displayed for the selected disk.
filesys	(Optional) Specifies that file system information be displayed for the selected disk.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2	This command was introduced in a release prior to Cisco IOS Release 12.2.
12.3	A timestamp that shows the offset from Coordinated Universal Time (UTC) was added to the **show disk** command display.
12.3(7)T	This command was enhanced to display information about the ATA ROM monitor library (monlib) file.

Usage Guidelines

The **show disk** command is supported only on platforms that have a disk file system.

Note The name of the ATA monlib file may contain a platform name that does not match the platform that you are using. Different platforms may have a similar or the same name for their ATA monlib file.

Examples

The following is sample output from the **show disk0** command:

```
Router# show disk0

-#- --length-- ---------date/time--------- path
1     21215616 Jun 24 2004 14:31:14 -08:00 c7200-g5js-mz.123-4.T1.bin
2     14209612 Jun 21 2004 13:20:34 -08:00 c7200-g5js-mz.122-13
3      3125832 Jun 23 2004 01:23:22 -08:00 c7200-boot-mz.120-18.S
4      2534764 Jun 23 2004 01:33:00 -08:00 c7200-boot-mz.120-28a.bin
5      3679928 Jun 23 2004 02:09:34 -08:00 c7200-boot-mz.120-28.S.bin
```

Table 53 describes the significant fields shown in the output.

Table 53 show disk Command Field Descriptions

Field	Description
#	Index number of the file on the disk.
length	Size of the file on the disk.
date/time	Last modification date. The time includes a conversion to local time in hours from Coordinated Universal Time (UTC). In the example, -08:00 indicates that the given time is 8 hours behind UTC or Pacific Standard Time (PST).
path	Name of the file.

The following is sample output from the **show disk0 all** command. The output is self-explanatory.

```
Router# show disk0 all

-#- --length-- ---------date/time--------- path
1     19539160 Jan 27 2004 23:08:40 -08:00 c7200-is-mz.123-5.7.PI3a

1011679232 bytes available (19546112 bytes used)

******** ATA Flash Card Geometry/Format Info ********

ATA CARD GEOMETRY
   Number of Heads:      16
   Number of Cylinders    1999
   Sectors per Track      63
   Sector Size            512
   Total Sectors          2014992
ATA CARD FORMAT
Number of FAT Sectors  246
   Sectors Per Cluster    32
   Number of Clusters     62941
   Number of Data Sectors 2014789
   Base Root Sector       632
   Base FAT Sector        140
   Base Data Sector       664

ATA MONLIB INFO
   Image Monlib size = 67256
   Disk monlib size = 71680
   Name = c7200-atafslib-m
   Monlib Start sector = 2
   Monlib End sector = 133
   Monlib updated by = C7200-IS-M12.3(5.7)PI3a
   Monlib version = 1
```

show environment

To display temperature, voltage, and blower information on the Cisco 7000 series, Cisco 7200 series, Cisco 7500 series routers, Cisco AS5300 series access servers, and Cisco 12000 series Gigabit Switch Routers (GSRs), use the **show environment** command in privileged EXEC mode.

show environment [**alarms** | **all** | **fans** | **hardware** | **last** | **leds** | **power-supply** | **table** | **temperature** | **voltages**]

Syntax Description

alarms	(Optional) Displays the alarm contact information.
all	(Optional) Displays a detailed listing of all environmental monitor parameters (for example, the power supplies, temperature readings, voltage readings, and blower speeds). This is the default.
fans	(Optional) Displays blower and fan information.
hardware	(Optional) Displays hardware-specific information.
last	(Optional) Displays information on the last measurement made.
leds	(Optional) Displays the status of the MBus LEDs on the clock and scheduler cards and switch fabric cards.
power-supply	(Optional) Displays power supply voltage and current information. If applicable, displays the status of the redundant power supply.
table	(Optional) Displays the temperature, voltage, and blower ranges and thresholds.
temperature	(Optional) Displays temperature information.
voltages	(Optional) Displays voltage information.

Defaults

If no options are specified, the default is **all**.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
11.2 GS	The **alarms**, **fans**, **hardware**, **leds**, **power-supply**, **table temperature,** and **voltages** keywords were added for Cisco 12000 series GSRs.
11.3(6)AA	This command was expanded to monitor the RPS and board temperature for the Cisco AS5300 platform, Cisco 3600 Series routers, Cisco 7200 series routers, and the Cisco 12000 series routers.

Usage Guidelines

The availability of keywords will depend on your system.

Once a minute a routine is run that gets environmental measurements from sensors and stores the output into a buffer. This buffer is displayed on the console when the **show environment** command is entered.

If a measurement exceeds desired margins, but has not exceeded fatal margins, a warning message is printed to the system console. The system software queries the sensors for measurements once a minute, but warnings for a given test point are printed at most once every hour for sensor readings in the warning range and once every 5 minutes for sensor readings in the critical range. If a measurement is out of line within these time segments, an automatic warning message appears on the console. As noted, you can query the environmental status with the **show environment** command at any time to determine whether a measurement is at the warning or critical tolerance.

If a shutdown occurs because of detection of fatal environmental margins, the last measured value from each sensor is stored in internal nonvolatile memory.

For environmental specifications, refer to the hardware installation and configuration publication for your individual chassis.

If the Cisco 12000 series exceeds environmental conditions, a message similar to the following is displayed on the console:

```
%GSR_ENV-2-WARNING: Slot 3 Hot Sensor Temperature exceeds 40 deg C;
Check cooling systems
```

Note Blower temperatures that exceed environmental conditions do not generate a warning message.

You can also enable Simple Network Management Protocol (SNMP) notifications (traps or informs) to alert a network management system (NMS) when environmental thresholds are reached using the **snmp-server enable traps envmon** and **snmp-server host** global configuration commands.

Whenever Cisco IOS software detects a failure or recovery event from the DRPS unit, it sends an SNMP trap to the configured SNMP server. Unlike console messages, only one SNMP trap is sent when the failure event is first detected. Another trap is sent when the recovery is detected.

Cisco AS5300 DRPS software reuses the MIB attributes and traps defined in CISCO-ENVMON-MIB and CISCO-ACCESS-ENVMON-MIB. CISCO-ENVMON-MIB is supported by all Cisco routers with RPS units, and CISCO-ACCESS-ENVMON-MIB is supported by the Cisco 3600 series routers.

A power supply trap defined in CISCO-ENVMON-MIB is sent when a failure is detected and when a failure recovery occurs for the following events: input voltage fail, DC output voltage fail, thermal fail, and multiple failure events.

A fan failure trap defined in CISCO-ENVMON-MIB is sent when a fan failure or recovery event is detected by Cisco IOS software.

A temperature trap defined in CISCO-ACCESS-ENVMON-MIB is sent when a board overtemperature condition is detected by Cisco IOS software.

CISCO-ACCESS-ENVMON-MIB also defines an overvoltage trap. A similar trap is defined in CISCO-ENVMON-MIB, but it requires the ciscoEnvMonVoltageStatusValue in varbinds. This value indicates the current value of the voltage in the RPS. With Cisco AS5300 RPS units, the current voltage value is not sent to the motherboard.

CISCO-ENVMON-MIB is extended to add a new enumerated value, internalRedundant(5), for MIB attribute ciscoEnvMonSupplySource. This is used to identify a RPS unit.

Examples

In the following example, the typical **show environment** display is shown when no warning conditions are in the system for the Cisco 7000 series and Cisco 7200 series routers. This information may vary slightly depending on the platform you are using. The date and time of the query are displayed, along with the data refresh information and a message indicating that there are no warning conditions.

```
Router> show environment

Environmental Statistics
  Environmental status as of 13:17:39 UTC Thu Jun 6 1996
  Data is 7 second(s) old, refresh in 53 second(s)

  All Environmental Measurements are within specifications
```

Table 54 describes the significant fields shown in the display.

Table 54 show environment Field Descriptions

Field	Description
Environmental status as of...	Current date and time.
Data is..., refresh in...	Environmental measurements are output into a buffer every 60 seconds, unless other higher-priority processes are running.
Status message	If environmental measurements are not within specification, warning messages are displayed.

Cisco 7000 Series Routers

The following are examples of messages that display on the system console when a measurement has exceeded an acceptable margin:

```
ENVIRONMENTAL WARNING: Air flow appears marginal.
ENVIRONMENTAL WARNING: Internal temperature measured 41.3(C)
ENVIRONMENTAL WARNING: +5 volt testpoint measured 5.310(V)
```

The system displays the following message if voltage or temperature exceed maximum margins:

```
SHUTDOWN: air flow problem
```

In the following example, there have been two intermittent power failures since a router was turned on, and the lower power supply is not functioning. The last intermittent power failure occurred on Monday, June 10, 1996, at 11:07 p.m.

```
7000# show environment all

Environmental Statistics
  Environmental status as of 23:19:47 UTC Wed Jun 12 1996
  Data is 6 second(s) old, refresh in 54 second(s)

  WARNING: Lower Power Supply is NON-OPERATIONAL

  Lower Power Supply:700W, OFF     Upper Power Supply: 700W, ON

  Intermittent Powerfail(s): 2     Last on 23:07:05 UTC Mon Jun 10 1996

  +12 volts measured at  12.05(V)
   +5 volts measured at   4.96(V)
  -12 volts measured at -12.05(V)
  +24 volts measured at  23.80(V)

  Airflow temperature measured at 38(C)
  Inlet temperature measured at 25(C)
```

Table 55 describes the significant fields shown in the display.

Table 55 show environment all Field Descriptions for the Cisco 7000 Series Routers

Field	Description
Environmental status as of...	Date and time of last query.
Data is..., refresh in...	Environmental measurements are output into a buffer every 60 seconds, unless other higher-priority processes are running.
WARNING:	If environmental measurements are not within specification, warning messages are displayed.
Lower Power Supply	Type of power supply installed and its status (On or Off).
Upper Power Supply	Type of power supply installed and its status (On or Off).
Intermittent Powerfail(s)	Number of power hits (not resulting in shutdown) since the system was last booted.
voltage specifications	System voltage measurements.
Airflow and inlet temperature	Temperature of air coming in and going out.

The following example is for the Cisco 7000 series router. The router retrieves the environmental statistics at the time of the last shutdown. In this example, the last shutdown was Friday, May 19, 1995, at 12:40 p.m., so the environmental statistics at that time are displayed.

```
Router# show environment last

Environmental Statistics
  Environmental status as of 14:47:00 UTC Sun May 21 1995
  Data is 6 second(s) old, refresh in 54 second(s)

  WARNING: Upper Power Supply is NON-OPERATIONAL

LAST Environmental Statistics
  Environmental status as of 12:40:00 UTC Fri May 19 1995
  Lower Power Supply: 700W, ON     Upper Power Supply: 700W, OFF

  No Intermittent Powerfails

  +12 volts measured at  12.05(V)
   +5 volts measured at   4.98(V)
  -12 volts measured at -12.00(V)
  +24 volts measured at  23.80(V)

 Airflow temperature measured at 30(C)
  Inlet  temperature measured at 23(C)
```

Table 56 describes the significant fields shown in the display.

Table 56 show environment last Field Descriptions for the Cisco 7000 Series Routers

Field	Description
Environmental status as of...	Current date and time.
Data is..., refresh in...	Environmental measurements are output into a buffer every 60 seconds, unless other higher-priority processes are running.

Table 56 show environment last Field Descriptions for the Cisco 7000 Series Routers (continued)

Field	Description
WARNING:	If environmental measurements are not within specification, warning messages are displayed.
LAST Environmental Statistics	Displays test point values at time of the last environmental shutdown.
Lower Power Supply: Upper Power Supply:	For the Cisco 7000 router, indicates the status of the two 700W power supplies. For the Cisco 7010 router, indicates the status of the single 600W power supply.

In the following example, shows sample output for the current environmental status in tables that list voltage and temperature parameters. There are three warning messages: one each about the lower power supply, the airflow temperature, and the inlet temperature. In this example, voltage parameters are shown to be in the normal range, airflow temperature is at a critical level, and inlet temperature is at the warning level.

```
Router> show environment table

Environmental Statistics
  Environmental status as of Mon 11-2-1992 17:43:36
  Data is 52 second(s) old, refresh in 8 second(s)

  WARNING: Lower Power Supply is NON-OPERATIONAL
  WARNING: Airflow temperature has reached CRITICAL level at 73(C)
  WARNING: Inlet temperature has reached WARNING level at 41(C)

Voltage Parameters:

 SENSE        CRITICAL                NORMAL                CRITICAL
-------|--------------------|------------------------|--------------------

+12(V)                 10.20        12.05(V)       13.80
 +5(V)                  4.74         4.98(V)        5.26
-12(V)                -10.20       -12.05(V)      -13.80
+24(V)                 20.00        24.00(V)       28.00

Temperature Parameters:

 SENSE     WARNING      NORMAL      WARNING      CRITICAL      SHUTDOWN
-------|-------------|------------|-------------|--------------|-----------

Airflow            10           60            70    73(C)       88
Inlet              10           39          41(C)   46          64
```

Table 57 describes the significant fields shown in the display.

Table 57 show environment Field Descriptions for the Cisco 7000 Series Router

Field	Description
SENSE (Voltage Parameters)	Voltage specification for a DC line.
SENSE (Temperature Parameters)	Air being measured. Inlet measures the air coming in, and Airflow measures the temperature of the air inside the chassis.
WARNING	System is approaching an out-of-tolerance condition.

Table 57 show environment Field Descriptions for the Cisco 7000 Series Router (continued)

Field	Description
NORMAL	All monitored conditions meet normal requirements.
CRITICAL	Out-of-tolerance condition exists.
SHUTDOWN	Processor has detected condition that could cause physical damage to the system.

Cisco 7200 Series Routers

The system displays the following message if the voltage or temperature enters the "Warning" range:

```
%ENVM-4-ENVWARN: Chassis outlet 3 measured at 55C/131F
```

The system displays the following message if the voltage or temperature enters the "Critical" range:

```
%ENVM-2-ENVCRIT: +3.45 V measured at +3.65 V
```

The system displays the following message if the voltage or temperature exceeds the maximum margins:

```
%ENVM-0-SHUTDOWN: Environmental Monitor initiated shutdown
```

The following message is sent to the console if a power supply has been inserted or removed from the system. This message relates only to systems that have two power supplies.

```
%ENVM-6-PSCHANGE: Power Supply 1 changed from Zytek AC Power Supply to removed
```

The following message is sent to the console if a power supply has been powered on or off. In the case of the power supply being shut off, this message can be due to the user shutting off the power supply or to a failed power supply. This message relates only to systems that have two power supplies.

```
%ENVM-6-PSLEV: Power Supply 1 state changed from normal to shutdown
```

The following is sample output from the **show environment all** command on the Cisco 7200 series router when there is a voltage warning condition in the system:

```
7200# show environment all

Power Supplies:
        Power supply 1 is unknown. Unit is off.
        Power supply 2 is Zytek AC Power Supply. Unit is on.

Temperature readings:
        chassis inlet    measured at 25C/77F
        chassis outlet 1 measured at 29C/84F
        chassis outlet 2 measured at 36C/96F
        chassis outlet 3 measured at 44C/111F
Voltage readings:
        +3.45 V measured at +3.83 V:Voltage in Warning range!
        +5.15 V measured at +5.09 V
        +12.15  measured at +12.42 V
        -11.95  measured at -12.10 V
```

Table 58 describes the significant fields shown in the display.

Table 58 show environment all Field Descriptions for the Cisco 7200 Series Router

Field	Description
Power Supplies:	Current condition of the power supplies including the type and whether the power supply is on or off.
Temperature readings:	Current measurements of the chassis temperature at the inlet and outlet locations.
Voltage readings:	Current measurement of the power supply test points.

The following example is for the Cisco 7200 series router. This example shows the measurements immediately before the last shutdown and the reason for the last shutdown (if appropriate).

```
7200# show environment last

   chassis inlet      previously measured at 27C/80F
   chassis outlet 1   previously measured at 31C/87F
   chassis outlet 2   previously measured at 37C/98F
   chassis outlet 3   previously measured at 45C/113F
   +3.3 V             previously measured at 4.02
   +5.0 V             previously measured at 4.92
   +12.0 V            previously measured at 12.65
   -12.0 V            previously measured at 11.71

last shutdown reason - power supply shutdown
```

Table 59 describes the significant fields shown in the display.

Table 59 show environment last Field Descriptions for the Cisco 7200 Series Router

Field	Description
chassis inlet	Temperature measurements at the inlet area of the chassis.
chassis outlet	Temperature measurements at the outlet areas of the chassis.
voltages	Power supply test point measurements.
last shutdown reason	Possible shutdown reasons are power supply shutdown, critical temperature, and critical voltage.

The following example is for the Cisco 7200 series router. This information lists the temperature and voltage shutdown thresholds for each sensor.

```
7200# show environment table

Sample Point      LowCritical    LowWarning     HighWarning    HighCritical
chassis inlet                                   40C/104F       50C/122F
chassis outlet 1                                43C/109F       53C/127F
chassis outlet 2                                75C/167F       75C/167F
chassis outlet 3                                55C/131F       65C/149F
+3.45 V           +2.76          +3.10          +3.80          +4.14
+5.15 V           +4.10          +4.61          +5.67          +6.17
+12.15 V          +9.72          +10.91         +13.37         +14.60
-11.95 V          -8.37          -9.57          -14.34         -15.53
Shutdown system at 70C/158F
```

Table 60 describes the significant fields shown in the display.

Table 60 show environment table Field Descriptions for the Cisco 7200 Series Router

Field	Description
Sample Point	Area for which measurements are taken.
LowCritical	Level at which a critical message is issued for an out-of-tolerance voltage condition. The system continues to operate; however, the system is approaching shutdown.
LowWarning	Level at which a warning message is issued for an out-of-tolerance voltage condition. The system continues to operate, but operator action is recommended to bring the system back to a normal state.
HighWarning	Level at which a warning message is issued. The system continues to operate, but operator action is recommended to bring the system back to a normal state.
HighCritical	Level at which a critical message is issued. For the chassis, the router is shut down. For the power supply, the power supply is shut down.
Shutdown system at	The system is shut down if the specified temperature is met.

Cisco 7500 Series Router

The sample output for the Cisco 7500 series routers may vary depending on the specific model (for example, the Cisco 7513 router). The following is sample output from the **show environment all** command on the Cisco 7500 series router:

```
7500# show environment all

Arbiter type 1, backplane type 7513 (id 2)
Power supply #1 is 1200W AC (id 1), power supply #2 is removed (id 7)
Active fault conditions: none
Fan transfer point: 100%
Active trip points: Restart_Inhibit
15 of 15 soft shutdowns remaining before hard shutdown

                        1
              0123456789012
Dbus slots:   X     XX    X

card        inlet      hotpoint      exhaust
RSP(6)     35C/95F     47C/116F      40C/104F
RSP(7)     35C/95F     43C/109F      39C/102F

Shutdown temperature source is 'hotpoint' on RSP(6), requested RSP(6)

+12V measured at 12.31
+5V measured at 5.21
-12V measured at -12.07
+24V measured at 22.08
+2.5 reference is 2.49

PS1 +5V Current      measured at 59.61 A (capacity 200 A)
PS1 +12V Current     measured at 5.08 A (capacity 35 A)
PS1 -12V Current     measured at 0.42 A (capacity 3 A)
PS1 output is 378 W
```

Table 61 describes the significant fields shown in the display.

Table 61 show environment all Field Descriptions for the Cisco 7500 Series Routers

Field	Description
Arbiter type 1	Numbers indicating the arbiter type and backplane type.
Power supply	Number and type of power supply installed in the chassis.
Active fault conditions:	Lists any fault conditions that exist (such as power supply failure, fan failure, and temperature too high).
Fan transfer point:	Software controlled fan speed. If the router is operating below its automatic restart temperature, the transfer point is reduced by 10 percent of the full range each minute. If the router is at or above its automatic restart temperature, the transfer point is increased in the same way.
Active trip points:	Compares temperature sensor against the values displayed at the bottom of the **show environment table** command output.
15 of 15 soft shutdowns remaining	When the temperature increases above the "board shutdown" level, a soft shutdown occurs (that is, the cards are shut down, and the power supplies, fans, and CI continue to operate). When the system cools to the restart level, the system restarts. The system counts the number of times this occurs and keeps the up/down cycle from continuing forever. When the counter reaches zero, the system performs a hard shutdown, which requires a power cycle to recover. The soft shutdown counter is reset to its maximum value after the system has been up for 6 hours.
Dbus slots:	Indicates which chassis slots are occupied.
card, inlet, hotpoint, exhaust	Temperature measurements at the inlet, hotpoint, and exhaust areas of the card. The (6) and (7) indicate the slot numbers. Dual-Route/Switch Processor (RSP) chassis can show two RSPs.
Shutdown temperature source	Indicates which of the three temperature sources is selected for comparison against the "shutdown" levels listed with the **show environment table** command.
Voltages (+12V, +5V, -12V, +24V, +2.5)	Voltages measured on the backplane.
PS1	Current measured on the power supply.

The following example is for the Cisco 7500 series router. This example shows the measurements immediately before the last shutdown.

```
7500# show environment last

 RSP(4) Inlet       previously measured at 37C/98F
 RSP(4) Hotpoint    previously measured at 46C/114F
 RSP(4) Exhaust     previously measured at 52C/125F
 +12 Voltage        previously measured at 12.26
 +5 Voltage         previously measured at 5.17
 -12 Voltage        previously measured at -12.03
 +24 Voltage        previously measured at 23.78
```

Table 62 describes the significant fields shown in the display.

Table 62 show environment last Field Descriptions for the Cisco 7500 Series Router

Field	Description
RSP(4) Inlet, Hotpoint, Exhaust	Temperature measurements at the inlet, hotpoint, and exhaust areas of the card.
Voltages	Voltages measured on the backplane.

The following example is for the Cisco 7500 series router. This information lists the temperature and voltage thresholds for each sensor. These thresholds indicate when error messages occur. There are two level of messages: warning and critical.

```
7500# show environment table

Sample Point      LowCritical    LowWarning     HighWarning    HighCritical
RSP(4) Inlet                                    44C/111F       50C/122F
RSP(4) Hotpoint                                 54C/129F       60C/140F
RSP(4) Exhaust
+12 Voltage       10.90          11.61          12.82          13.38
+5 Voltage        4.61           4.94           5.46           5.70
-12 Voltage       -10.15         -10.76         -13.25         -13.86
+24 Voltage       20.38          21.51          26.42          27.65
2.5 Reference                    2.43           2.51
Shutdown boards at           70C/158F
Shutdown power supplies at   76C/168F
Restart after shutdown below 40C/104F
```

Table 63 describes the significant fields shown in the display.

Table 63 show environment table Field Descriptions for the Cisco 7500 Series Router

Field	Description
Sample Point	Area for which measurements are taken.
LowCritical	Level at which a critical message is issued for an out-of-tolerance voltage condition. The system continues to operate; however, the system is approaching shutdown.
LowWarning	Level at which a warning message is issued for an out-of-tolerance voltage condition. The system continues to operate, but operator action is recommended to bring the system back to a normal state.
HighWarning	Level at which a warning message is issued. The system continues to operate, but operator action is recommended to bring the system back to a normal state.
HighCritical	Level at which a critical message is issued. For the chassis, the router is shut down. For the power supply, the power supply is shut down.
Shutdown boards at	The card is shut down if the specified temperature is met.
Shutdown power supplies at	The system is shut down if the specified temperature is met.
Restart after shutdown	The system will restart when the specified temperature is met.

Cisco AS5300 Series Access Servers

In the following example, keywords and options are limited according to the physical characteristics of the system is shown:

```
as5300# show environment ?

  all    All environmental monitor parameters
  last   Last environmental monitor parameters
  table  Temperature and voltage ranges
  |      Output modifiers
  <cr>

as5300# show environment table

%This option not available on this platform
```

Cisco 12000 Series GSR

The following examples are for the Cisco 12000 series GSRs.

The following is sample output from the **show environment** command for a Cisco 12012 router. Slots 0 through 11 are the line cards, slots 16 and 17 are the clock and scheduler cards, slots 18 through 20 are the switch fabric cards, slots 24 through 26 are the power supplies, and slots 28 and 29 are the blowers. An “NA” in the table means that no values were returned. In some cases it is because the equipment is not supported for that environmental parameter (for example, the power supply and blowers in slots 24, 26, 28, and 29 do not have a 3V power supply, so an NA is displayed).

```
Router# show environment

Slot #  3V      5V      MBUS 5V Hot Sensor      Inlet Sensor
        (mv)    (mv)    (mv)     (deg C)          (deg C)
0       3300    4992    5040       42.0           37.0
2       3296    4976    5136       40.0           33.0
4       3280    4992    5120       38.5           31.5
7       3280    4984    5136       42.0           32.0
9       3292    4968    5160       39.5           31.5
11      3288    4992    5152       40.0           30.5
16      3308    NA      5056       42.5           38.0
17      3292    NA      5056       40.5           36.5
18      3304    NA      5176       36.5           35.0
19      3300    NA      5184       37.5           33.5
20      3304    NA      5168       36.5           34.0
24      NA      5536    5120       NA             31.5
26      NA      5544    5128       NA             31.5
28      NA      NA      5128       NA             NA
29      NA      NA      5104       NA             NA

Slot #  48V     AMP_48
        (Volt)  (Amp)
24      46      12
26      46      19

Slot #  Fan 0   Fan 1   Fan 2
        (RPM)   (RPM)   (RPM)
28      2160    2190    2160
29      2130    2190    2070
Router#
```

Table 64 describes the significant fields shown and lists the equipment supported by each environmental parameter. “NA” indicates that the reading could not be obtained, so the command should be again.

Table 64 show environment Field Descriptions for the Cisco 12000 Series Routers

Field	Description
Slot #	Slot number of the equipment. On the Cisco 12012 router, slots 0 through 11 are the line cards, slots 16 and 17 are the clock and scheduler cards, slots 18 through 20 are the switch fabric cards, slots 24 through 27 are the power supplies, and slots 28 and 29 are the blowers.
3V (mv)	Measures the 3v power supply on the card. The 3v power supply is on the line cards, GRP card, clock and scheduler cards, and switch fabric cards.
5V (mv)	Measures the 5v power supply on the card. The 5v power supply is on the line cards, GRP card, and power supplies.
MBUS 5V (mv)	Measures the 5v MBus on the card. The 5v MBus is on all equipment.
Hot Sensor (deg C)	Measures the temperature at the hot sensor on the card. The hot sensor is on the line cards, GRP card, clock and scheduler cards, switch fabric cards, and blowers.
Inlet Sensor (deg C)	Measures the current inlet temperature on the card. The inlet sensor is on the line cards, GRP card, clock and scheduler cards, switch fabric cards, and power supplies.
48V (Volt)	Measures the DC power supplies.
AMP_48 (Amp)	Measures the AC power supplies.
Fan 0, Fan 1, Fan 2	Measures the fan speed in rotations per minute.

The following is sample output from the **show environment all** command for the Cisco 12008 router. Slots 0 through 7 are the line cards, slots 16 and 17 are the clock scheduler cards (the clock scheduler cards control the fans), slots 18 through 20 are the switch fabric cards, and slots 24 and 26 are the power supplies. The Cisco 12008 router does not support slots 25, 27, 28, and 29. An "NA" in the table means that no values were returned. In some cases it is because the equipment is not supported for that environmental parameter (for example, the power supplies in slots 24 and 26 do not have a hot sensor, so an NA is displayed).

```
Router# show environment all

Slot #  Hot Sensor      Inlet Sensor
         (deg C)          (deg C)
2          31.0            22.0
5          33.5            26.5
16         25.5            21.5
18         22.0            21.0
19         22.5            21.0
24         NA              29.5
26         NA              24.5

Slot #  3V      5V      MBUS 5V
        (mv)    (mv)    (mv)
2       3292    5008    5136
5       3292    5000    5128
16      3272    NA      5128
18      3300    NA      5128
19      3316    NA      5128


Slot #  5V      MBUS 5V 48V     AMP_48
        (mv)    (mv)    (Volt)  (Amp)
```

```
24      0       5096    3       0
26      5544    5144    47      3

Slot #  Fan Information
16      Voltage 16V Speed slow: Main Fans Ok Power Supply fans Ok

Alarm Indicators
No alarms

Slot #  Card Specific Leds
16      Mbus OK SFCs Failed
18      Mbus OK
19      Mbus OK
24      Input Failed
26      Input Ok
```

The following is sample output from the **show environment table** command for a Cisco 12012 router. The **show environment table** command lists the warning, critical, and shutdown limits on your system and includes the GRP card and line cards (slots 0 to 15), clock and scheduler cards (slots 16 and 17), switch fabric cards (slots 18 to 20), and blowers.

```
Router# show environment table

Hot Sensor Temperature Limits (deg C):
                        Warning Critical Shutdown
GRP/GLC (Slots 0-15)       40      46      57
CSC     (Slots 16-17)      46      51      65
SFC     (Slots 18-20)      41      46      60

Inlet Sensor Temperature Limits (deg C):
                        Warning Critical Shutdown
GRP/GLC (Slots 0-15)       35      40      52
CSC     (Slots 16-17)      40      45      59
SFC     (Slots 18-20)      37      42      54

3V Ranges (mv):
                           Warning         Critical        Shutdown
                        Below   Above    Below  Above    Below  Above
GRP/GLC (Slots 0-15)     3200    3400     3100   3500     3050   3550
CSC     (Slots 16-17)    3200    3400     3100   3500     3050   3550
SFC     (Slots 18-20)    3200    3400     3100   3500     3050   3550

5V Ranges (mv):
                           Warning         Critical        Shutdown
                        Below   Above    Below  Above    Below  Above
GRP/GLC (Slots 0-15)     4850    5150     4750   5250     4680   5320

MBUS_5V Ranges (mv):
                           Warning         Critical        Shutdown
                        Below   Above    Below  Above    Below  Above
GRP/GLC (Slots 0-15)     5000    5250     4900   5350     4750   5450
CSC     (Slots 16-17)    4820    5150     4720   5250     4750   5450
SFC     (Slots 17-20)    5000    5250     4900   5350     4750   5450


Blower Operational Range (RPM):

Top Blower:
               Warning    Critical
                Below      Below
Fan 0          1000        750
Fan 1          1000        750
Fan 2          1000        750
```

```
Bottom Blower:
                Warning    Critical
                 Below      Below
Fan 0           1000        750
Fan 1           1000        750
Fan 2           1000        750
```

The following is sample output from the **show environment leds** command for a Cisco 12012 router. The **show environment leds** command lists the status of the MBus LEDs on the clock, scheduler, and the switch fabric cards.

```
Router# show environment leds

16 leds Mbus OK
18 leds Mbus OK
19 leds Mbus OK
20 leds Mbus OK
```

Related Commands

Command	Description
snmp-server enable traps envmon	Controls (enables or disables) environmental monitoring SNMP notifications.
snmp-server host	Specifies how SNMP notifications should be sent (as traps or informs), the version of SNMP to use, the security level of the notifications (for SNMPv3), and the recipient (host) of the notifications.

show file

The **show file** command has been replaced by the **more** command. See the description of the **more** command for more information.

show file descriptors

To display a list of open file descriptors, use the **show file descriptors** command in EXEC mode.

show file descriptors

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.

Usage Guidelines

File descriptors are the internal representations of open files. You can use this command to learn if another user has a file open.

Examples

The following is sample output from the **show file descriptors** command:

```
Router# show file descriptors

File Descriptors:

   FD  Position  Open  PID  Path
    0    187392  0001    2  tftp://dirt/hampton/c4000-i-m.a
    1    184320  030A    2  flash:c4000-i-m.a
```

Table 65 describes the fields shown in the display.

Table 65 show file descriptors Field Descriptions

Field	Description
FD	File descriptor. The file descriptor is a small integer used to specify the file once it has been opened.
Position	Byte offset from the start of the file.
Open	Flags supplied when opening the file.
PID	Process ID of the process that opened the file.
Path	Location of the file.

show file information

To display information about a file, use the **show file information** command in EXEC mode.

show file information *file-url*

Syntax Description

file-url	The URL of the file to display.

Command Modes

EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.

Examples

The following is sample output from the **show file information** command:

```
Router# show file information tftp://dirt/hampton/c2500-j-l.a

tftp://dirt/hampton/c2500-j-l.a:
  type is image (a.out) [relocatable, run from flash]
  file size is 8624596 bytes, run size is 9044940 bytes [8512316+112248+420344]
  Foreign image

Router# show file information slot0:c7200-js-mz

slot0:c7200-js-mz:
  type is image (elf) []
  file size is 4770316 bytes, run size is 4935324 bytes
  Runnable image, entry point 0x80008000, run from ram

Router1# show file information nvram:startup-config

nvram:startup-config:
  type is ascii text
```

Table 66 describes the possible file types.

Table 66 Possible File Types

Types	Description
image (a.out)	Runnable image in a.out format.
image (elf)	Runnable image in elf format.
ascii text	Configuration file or other text file.
coff	Runnable image in coff format.
ebcdic	Text generated on an IBM mainframe.
lzw compression	Lzw compressed file.
tar	Text archive file used by the Channel Interface Processor (CIP).

show file systems

To list available file systems, use the **show file systems** command in EXEC mode.

show file systems

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.

Usage Guidelines

Use this command to learn the alias names (Prefixes) of the file systems your router supports.

Examples

The following is sample output from the **show file systems** command:

```
Router# show file systems

File Systems:

     Size(b)         Free(b)   Type     Flags  Prefixes
           -               -    opaque     rw     null:
           -               -    opaque     rw     system:
           -               -    opaque     ro     xmodem:
           -               -    opaque     ro     ymodem:
           -               -   network     rw     tftp:
           -               -   network     rw     rcp:
           -               -   network     rw     ftp:
*    4194304         4190616     flash     rw     flash:
      131066          129185     nvram     rw     nvram:
           -               -    opaque     wo     lex:
```

Table 67 describes the significant fields shown in the display.

Table 67 show file systems Field Descriptions

Type	Description
Size(b)	Amount of memory in the file system (in bytes).
Free(b)	Amount of free memory in the file system (in bytes).
Type	Type of file system.
Flags	Permissions for file system.
Prefixes	Alias for file system.
disk	The file system is for a rotating medium.
flash	The file system is for a Flash memory device.

Table 67 show file systems Field Descriptions (continued)

Type	Description
network	The file system is a network file system (TFTP, rcp, FTP, and so on).
nvram	The file system is for an NVRAM device.
opaque	The file system is a locally generated “pseudo” file system (for example, the “system”) or a download interface, such as brimux.
rom	The file system is for a ROM or EPROM device.
tty	The file system is for a collection of terminal devices.
unknown	The file system is of unknown type.

Table 68 describes file system flags.

Table 68 Possible File System Flags

Flag	Description
ro	The file system is Read Only.
rw	The file system is Write Only.
wo	The file system is Read/Write.

show (flash)

To display the layout and contents of a Flash memory file system, use the **show** *flash-filesystem* command in EXEC mode.

Class A Flash File Systems

show *flash-filesystem***:** [**all** | **chips** | **filesys**]

Class B Flash File Systems

show *flash-filesystem***:** [**partition** *number*] [**all** | **chips** | **detailed** | **err** | **summary**]

Class C Flash File Systems

show *flash-filesystem***:**

Syntax Description

flash-filesystem:	Flash memory file system followed by a colon. Valid flash file system keywords inlude: • **bootflash:** • **flash:** • **slot0:** • **slot1:** • **slavebootflash:** • **slaveslot0:** • **slaveslot1:**,
all	(Optional) On Class B Flash file systems, **all** keyword displays complete information about Flash memory, including information about the individual ROM devices in Flash memory and the names and sizes of all system image files stored in Flash memory, including those that are invalid. On Class A Flash file systems, the **all** keyword displays the following information: • The information displayed when no keywords are used. • The information displayed by the **filesys** keyword. • The information displayed by the **chips** keyword.
chips	(Optional) Displays information per partition and per chip, including which bank the chip is in, plus its code, size, and name.
filesys	(Optional) Displays the Device Info Block, the Status Info, and the Usage Info.
partition *number*	(Optional) Displays output for the specified partition number. If you do not specify a partition in the command, the router displays output for all partitions. You can use this keyword only when Flash memory has multiple partitions.

detailed	(Optional) Displays detailed file directory information per partition, including file length, address, name, Flash memory checksum, computer checksum, bytes used, bytes available, total bytes, and bytes of system Flash memory.
err	(Optional) Displays write or erase failures in the form of number of retries.
summary	(Optional) Displays summary information per partition, including the partition size, bank size, state, and method by which files can be copied into a particular partition. You can use this keyword only when Flash memory has multiple partitions.

Command Modes

EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.
12.3	A timestamp that shows the offset from Coordinated Universal Time (UTC) was added to the **show** command display.

Usage Guidelines

If Flash memory is partitioned, the command displays the requested output for each partition, unless you use the **partition** keyword.

The command also specifies the location of the current image.

To display the contents of boot Flash memory on Class A or B file systems, use the **show bootflash:** command as follows:

Class A Flash file systems

show bootflash: [**all** | **chips** | **filesys**]

Class B Flash file systems

show bootflash: [**partition** *number*] [**all** | **chips** | **detailed** | **err**]

To display the contents of internal Flash memory on Class A or B file systems, use the **show flash:** command as follows:

Class A Flash file systems

show flash: [**all** | **chips** | **filesys**]

Class B Flash file systems

show flash: [**partition** *number*][**all** | **chips** | **detailed** | **err** | **summary**]

The **show** (Flash file system) command replaces the **show flash devices** command.

Examples

The output of the **show** command depends on the type of Flash file system you select. Types include **flash:**, **bootflash:**, **slot0:**, **slot1:**, **slavebootflash:**, **slaveslot0:**, and **slaveslot1:**.

Examples of output from the **show flash** command are provided in the following sections:

- Class A Flash File System
- Class B Flash File Systems

Although the examples use **flash:** as the Flash file system, you may also use the other Flash file systems listed.

Class A Flash File System

The following three examples show sample output for Class A Flash file systems. Table 69 describes the significant fields shown in the display.

The following is sample output from the **show flash:** command.

```
Router# show flash:

-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1   .. unknown  317FBA1B  4A0694   24  4720148 Dec 15 2003 17:49:36 -08:00
hampton/nitro/c7200-j-mz
2   .. unknown  9237F3FF  92C574   11  4767328 Jan 02 2004 18:42:53 -08:00 c7200-js-mz
3   .D unknown  71AB01F1 10C94E0   10  7982828 Jan 02 2004 18:48:14 -08:00 rsp-jsv-mz
4   .D unknown  96DACD45 10C97E0    8      639 Jan 03 2004 12:09:17 -08:00 the_time
5   .. unknown  96DACD45 10C9AE0    3      639 Jan 03 2004 12:09:32 -08:00 the_time
6   .D unknown  96DACD45 10C9DE0    8      639 Jan 03 2004 12:37:01 -08:00 the_time
7   .. unknown  96DACD45 10CA0E0    8      639 Jan 03 2004 12:37:13 -08:00 the_time

3104544 bytes available (17473760 bytes used)
```

Table 69 show (Class A Flash File System) Field Descriptions

Field	Description
#	Index number for the file.
ED	Whether the file contains an error (*E*) or is deleted (*D*).
type	File type (1 = configuration file, 2 = image file). The software displays these values only when the file type is certain. When the file type is unknown, the system displays “unknown” in this field.
crc	Cyclic redundant check for the file.
seek	Offset into the file system of the next file.
nlen	Name length—Length of the filename.
length	Length of the file itself.
date/time	Date and time the file was created. In the example, -08:00 indicates that the given date and time is 8 hours behind Coordinated Universal Time (UTC).
name	Name of the file.

The following is sample output from the **show flash: chips** command:

```
RouterA# show flash: chips

******** Intel Series 2+ Status/Register Dump ********

ATTRIBUTE MEMORY REGISTERS:
  Config Option Reg (4000): 2
  Config Status Reg (4002): 0
  Card Status   Reg (4100): 1
```

```
  Write Protect Reg (4104): 4
  Voltage Cntrl Reg (410C): 0
  Rdy/Busy Mode Reg (4140): 2

COMMON MEMORY REGISTERS: Bank 0
  Intelligent ID Code  : 8989A0A0
  Compatible Status Reg: 8080
  Global     Status Reg: B0B0
  Block Status Regs:
    0  :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    8  :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    16 :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    24 :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0

COMMON MEMORY REGISTERS: Bank 1
  Intelligent ID Code  : 8989A0A0
  Compatible Status Reg: 8080
  Global     Status Reg: B0B0
  Block Status Regs:
    0  :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    8  :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    16 :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    24 :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0

COMMON MEMORY REGISTERS: Bank 2
  Intelligent ID Code  : 8989A0A0
  Compatible Status Reg: 8080
  Global     Status Reg: B0B0
  Block Status Regs:
    0  :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    8  :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    16 :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    24 :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0

COMMON MEMORY REGISTERS: Bank 3
  Intelligent ID Code  : 8989A0A0
  Compatible Status Reg: 8080
  Global     Status Reg: B0B0
  Block Status Regs:
    0  :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    8  :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    16 :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    24 :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0

COMMON MEMORY REGISTERS: Bank 4
  Intelligent ID Code  : 8989A0A0
  Compatible Status Reg: 8080
  Global     Status Reg: B0B0
  Block Status Regs:
    0  :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    8  :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    16 :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    24 :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
```

The following is sample output from the **show flash: filesys** command:

```
RouterA# show flash: filesys

-------- F I L E   S Y S T E M   S T A T U S --------
  Device Number = 0
DEVICE INFO BLOCK:
  Magic Number          = 6887635   File System Vers = 10000    (1.0)
  Length                = 1400000   Sector Size      = 20000
  Programming Algorithm = 4         Erased State     = FFFFFFFF
```

```
  File System Offset    = 20000     Length = 13A0000
  MONLIB Offset         = 100       Length = C730
  Bad Sector Map Offset = 1FFEC     Length = 14
  Squeeze Log Offset    = 13C0000   Length = 20000
  Squeeze Buffer Offset = 13E0000   Length = 20000
  Num Spare Sectors     = 0
    Spares:
STATUS INFO:
  Writable
  NO File Open for Write
  Complete Stats
  No Unrecovered Errors
  No Squeeze in progress
USAGE INFO:
  Bytes Used     = 10AA0E0  Bytes Available = 2F5F20
  Bad Sectors    = 0        Spared Sectors  = 0
  OK Files       = 4        Bytes = 90C974
  Deleted Files  = 3        Bytes = 79D3EC
  Files w/Errors = 0        Bytes = 0
```

The following is sample output from the **show flash:** command:

```
RouterB> show flash:

System flash directory:
File  Length   Name/status
  1   4137888  c3640-c2is-mz.Feb24
[4137952 bytes used, 12639264 available, 16777216 total]
16384K bytes of processor board System flash (Read/Write)\
```

The following example shows detailed information about the second partition in internal Flash memory:

```
RouterB# show flash: partition 2

System flash directory, partition 2:
File  Length   Name/status
  1   1711088  dirt/images/c3600-i-mz
[1711152 bytes used, 15066064 available, 16777216 total]
16384K bytes of processor board System flash (Read/Write)
```

Class B Flash File Systems

Table 70 describes the significant fields shown in the displays.

Table 70 show (Class B Flash File System) all Fields

Field	Description
addr	Address of the file in Flash memory.
available	Total number of bytes available in Flash memory.
Bank	Bank number.
Bank-Size	Size of bank in bytes.
bytes used	Total number of bytes used in Flash memory.
ccksum	Computed checksum.
Chip	Chip number.
Code	Code number.

Table 70 show (Class B Flash File System) all Fields (continued)

Field	Description
Copy-Mode	Method by which the partition can be copied to: • RXBOOT-MANUAL indicates a user can copy manually by reloading to the boot ROM image. • RXBOOT-FLH indicates user can copy via Flash load helper. • Direct indicates user can copy directly into Flash memory. • None indicates that it is not possible to copy into that partition.
fcksum	Checksum recorded in Flash memory.
File	Number of the system image file. If no filename is specified in the **boot system flash** command, the router boots the system image file with the lowest file number.
Free	Number of bytes free in partition.
Length	Size of the system image file (in bytes).
Name	Name of chip manufacturer and chip type.
Name/status	Filename and status of a system image file. The status [invalidated] appears when a file has been rewritten (recopied) into Flash memory. The first (now invalidated) copy of the file is still present within Flash memory, but it is rendered unusable in favor of the newest version. The [invalidated] status can also indicate an incomplete file that results from the user abnormally terminating the copy process, a network timeout, or a Flash memory overflow.
Partition	Partition number in Flash memory.
Size	Size of partition (in bytes) or size of chip.
State	State of the partition. It can be one of the following values: • Read-Only indicates the partition that is being executed from. • Read/Write is a partition that can be copied to.
System flash directory	Flash directory and its contents.
total	Total size of Flash memory (in bytes).
Used	Number of bytes used in partition.

The following is sample output from the **show flash: all** command:

```
RouterB> show flash: all
Partition   Size    Used      Free      Bank-Size  State          Copy Mode
  1        16384K   4040K    12343K     4096K      Read/Write     Direct

System flash directory:
File  Length   Name/status
        addr      fcksum  ccksum
  1   4137888  c3640-c2is-mz.Feb24
        0x40      0xED65  0xED65
```

```
[4137952 bytes used, 12639264 available, 16777216 total]
16384K bytes of processor board System flash (Read/Write)

   Chip    Bank    Code      Size      Name
    1      1       01D5      1024KB    AMD   29F080
    2      1       01D5      1024KB    AMD   29F080
    3      1       01D5      1024KB    AMD   29F080
    4      1       01D5      1024KB    AMD   29F080
    1      2       01D5      1024KB    AMD   29F080
    2      2       01D5      1024KB    AMD   29F080
    3      2       01D5      1024KB    AMD   29F080
    4      2       01D5      1024KB    AMD   29F080
    1      3       01D5      1024KB    AMD   29F080
    2      3       01D5      1024KB    AMD   29F080
    3      3       01D5      1024KB    AMD   29F080
    4      3       01D5      1024KB    AMD   29F080
    1      4       01D5      1024KB    AMD   29F080
    2      4       01D5      1024KB    AMD   29F080
    3      4       01D5      1024KB    AMD   29F080
    4      4       01D5      1024KB    AMD   29F080
```

The following is sample output from the **show flash: all** command on a router with Flash memory partitioned:

```
Router# show flash: all

System flash partition information:
Partition   Size    Used       Free     Bank-Size     State         Copy-Mode
    1       4096K    3459K     637K     4096K         Read Only     RXBOOT-FLH
    2       4096K    3224K     872K     4096K         Read/Write    Direct

System flash directory, partition 1:
File     Length     Name/status
        addr     fcksum     ccksum
  1     3459720     master/igs-bfpx.100-4.3
        0x40     0x3DE1     0x3DE1
[3459784 bytes used, 734520 available, 4194304 total]
4096K bytes of processor board System flash (Read ONLY)

   Chip    Bank     Code      Size      Name
    1      1        89A2      1024KB    INTEL 28F008SA
    2      1        89A2      1024KB    INTEL 28F008SA
    3      1        89A2      1024KB    INTEL 28F008SA
    4      1        89A2      1024KB    INTEL 28F008SA
Executing current image from System flash [partition 1]

 System flash directory, partition2:
File     Length     Name/status
        addr     fcksum     ccksum
  1     3224008     igs-kf.100
        0x40     0xEE91     0xEE91
[3224072 bytes used, 970232 available, 4194304 total]
4096K bytes of processor board System flash (Read/Write)

   Chip    Bank     Code      Size      Name
    1      2        89A2      1024KB    INTEL 28F008SA
    2      2        89A2      1024KB    INTEL 28F008SA
    3      2        89A2      1024KB    INTEL 28F008SA
    4      2        89A2      1024KB    INTEL 28F008SA
```

The following is sample output from the **show flash: chips** command:

```
RouterB> show flash: chips

16384K bytes of processor board System flash (Read/Write)

   Chip    Bank    Code      Size      Name
    1       1       01D5      1024KB    AMD   29F080
    2       1       01D5      1024KB    AMD   29F080
    3       1       01D5      1024KB    AMD   29F080
    4       1       01D5      1024KB    AMD   29F080
    1       2       01D5      1024KB    AMD   29F080
    2       2       01D5      1024KB    AMD   29F080
    3       2       01D5      1024KB    AMD   29F080
    4       2       01D5      1024KB    AMD   29F080
    1       3       01D5      1024KB    AMD   29F080
    2       3       01D5      1024KB    AMD   29F080
    3       3       01D5      1024KB    AMD   29F080
    4       3       01D5      1024KB    AMD   29F080
    1       4       01D5      1024KB    AMD   29F080
    2       4       01D5      1024KB    AMD   29F080
    3       4       01D5      1024KB    AMD   29F080
    4       4       01D5      1024KB    AMD   29F080
```

The following is sample output from the **show flash: detailed** command:

```
RouterB> show flash: detailed

System flash directory:
File  Length   Name/status
        addr      fcksum  ccksum
  1   4137888  c3640-c2is-mz.Feb24
        0x40      0xED65  0xED65
[4137952 bytes used, 12639264 available, 16777216 total]
16384K bytes of processor board System flash (Read/Write)
```

The following is sample output from the **show flash: err** command:

```
RouterB> show flash: err

System flash directory:
File  Length   Name/status
  1   4137888  c3640-c2is-mz.Feb24
[4137952 bytes used, 12639264 available, 16777216 total]
16384K bytes of processor board System flash (Read/Write)

   Chip    Bank    Code      Size      Name                erase  write
    1       1       01D5      1024KB    AMD   29F080        0      0
    2       1       01D5      1024KB    AMD   29F080        0      0
    3       1       01D5      1024KB    AMD   29F080        0      0
    4       1       01D5      1024KB    AMD   29F080        0      0
    1       2       01D5      1024KB    AMD   29F080        0      0
    2       2       01D5      1024KB    AMD   29F080        0      0
    3       2       01D5      1024KB    AMD   29F080        0      0
    4       2       01D5      1024KB    AMD   29F080        0      0
    1       3       01D5      1024KB    AMD   29F080        0      0
    2       3       01D5      1024KB    AMD   29F080        0      0
    3       3       01D5      1024KB    AMD   29F080        0      0
    4       3       01D5      1024KB    AMD   29F080        0      0
    1       4       01D5      1024KB    AMD   29F080        0      0
    2       4       01D5      1024KB    AMD   29F080        0      0
    3       4       01D5      1024KB    AMD   29F080        0      0
    4       4       01D5      1024KB    AMD   29F080        0      0
```

See Table 70 for a description of the fields. The **show flash: err** command also displays two extra fields: erase and write. The erase field indications the number of erase errors. The write field indicates the number of write errors.

The following is sample output from the **show flash summary** command on a router with Flash memory partitioned. The partition in the Read Only state is the partition from which the Cisco IOS image is being executed.

```
Router# show flash summary

System flash partition information:
Partition   Size     Used      Free    Bank-Size   State       Copy-Mode
    1       4096K    2048K     2048K   2048K       Read Only   RXBOOT-FLH
    2       4096K    2048K     2048K   2048K       Read/Write  Direct
```

Related Commands

Command	Description
more	Displays the contents of any file in the Cisco IOS File System.

show flh-log

The **show flh-log** command has been replaced by the **more flh:logfile** command. See the description of the **more flh:logfile** command for more information.

show gsr

To display hardware information on the Cisco 12000 series Gigabit Switch Routers (GSRs), use the **show gsr** command in EXEC mode.

show gsr [**chassis-info** [**details**]]

Syntax Description

chassis-info	(Optional) Displays backplane NVRAM information.
details	(Optional) In addition to the information displayed, this option includes hexadecimal output of the backplane NVRAM information.

Command Modes

EXEC

Command History

Release	Modification
11.2GS	This command was introduced to support the Cisco 12000 series GSRs.

Usage Guidelines

Use this command to determine the type of hardware installed in your Cisco 12000 series GSR router.

Examples

The following is sample output from the **show gsr** command for a Cisco 12012 router. This command shows the type and state of the card installed in the slot.

```
Router# show gsr

Slot 0  type  = Route Processor
        state = IOS Running  MASTER
Slot 7  type  = 1 Port Packet Over SONET OC-12c/STM-4c
        state = Card Powered
Slot 16 type  = Clock Scheduler Card
        state = Card Powered  PRIMARY CLOCK
```

The following is sample output from the **show gsr chassis-info** command for a Cisco 12012 router:

```
Router# show gsr chassis-info

Backplane NVRAM [version 0x20] Contents -
  Chassis: type 12012 Fab Ver: 1
    Chassis S/N: ZQ24CS3WT86MGVHL
  PCA: 800-3015-1  rev: A0  dev: 257  HW ver: 1.0
    Backplane S/N: A109EXPR75FUNYJK
  MAC Addr: base 0000.EAB2.34FF  block size: 1024
  RMA Number: 0x5F-0x2D-0x44  code: 0x01  hist: 0x1A
```

show gt64010 (7200)

To display all GT64010 internal registers and interrupt status on the Cisco 7200 series routers, use the **show gt64010** command in EXEC mode.

show gt64010

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command displays information about the CPU interface, DRAM/device address space, device parameters, direct memory access (DMA) channels, timers and counters, and protocol control information (PCI) internal registers. The information is generally useful for diagnostic tasks performed by technical support only.

Examples

The following is a partial sample output for the **show gt64010** command:

```
Router# show gt64010

GT64010 Channel 0 DMA:
 dma_list=0x6088C3EC, dma_ring=0x4B018480, dma_entries=256
 dma_free=0x6088CECC, dma_reqt=0x6088CECC, dma_done=0x6088CECC
 thread=0x6088CEAC, thread_end=0x6088CEAC
 backup_thread=0x0, backup_thread_end=0x0
 dma_working=0, dma_complete=6231, post_coalesce_frames=6231
 exhausted_dma_entries=0, post_coalesce_callback=6231

GT64010 Register Dump: Registers at 0xB4000000

CPU Interface:
 cpu_interface_conf   : 0x80030000 (b/s 0x00000380)
 addr_decode_err      : 0xFFFFFFFF (b/s 0xFFFFFFFF)
Processor Address Space :
 ras10_low            : 0x00000000 (b/s 0x00000000)
 ras10_high           : 0x07000000 (b/s 0x00000007)
 ras32_low            : 0x08000000 (b/s 0x00000008)
 ras32_high           : 0x0F000000 (b/s 0x0000000F)
 cs20_low             : 0xD0000000 (b/s 0x000000D0)
 cs20_high            : 0x74000000 (b/s 0x00000074)
 cs3_boot_low         : 0xF8000000 (b/s 0x000000F8)
 cs3_boot_high        : 0x7E000000 (b/s 0x0000007E)
 pci_io_low           : 0x00080000 (b/s 0x00000800)
 pci_io_high          : 0x00000000 (b/s 0x00000000)
 pci_mem_low          : 0x00020000 (b/s 0x00000200)
 pci_mem_high         : 0x7F000000 (b/s 0x0000007F)
 internal_spc_decode  : 0xA0000000 (b/s 0x000000A0)
```

```
 bus_err_low          : 0x00000000 (b/s 0x00000000)
 bus_err_high         : 0x00000000 (b/s 0x00000000)
.
.
.
```

show history

To list the commands you have entered in the current EXEC session, use the **show history** command in EXEC mode.

show history

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The command history feature provides a record of EXEC commands you have entered. The number of commands that the history buffer will record is determined by the **history size** line configuration command or the **terminal history size** EXEC command.

Table 71 lists the keys and functions you can use to recall commands from the command history buffer.

Table 71 History Keys

Key	Function
Ctrl-P or Up Arrow[1]	Recalls commands in the history buffer in a backward sequence, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Ctrl-N or Down Arrow[1]	Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow. Repeat the key sequence to recall successively more recent commands.

1. The arrow keys function only with ANSI-compatible terminals.

Examples

The following is sample output from the **show history** command, which lists the commands the user has entered in EXEC mode for this session:

```
Router# show history
  help
  where
  show hosts
  show history
Router#
```

Related Commands

Command	Description
history size	Enables the command history function, or changes the command history buffer size for a particular line.
terminal history size	Enables the command history feature for the current terminal session, or changes the size of the command history buffer for the current terminal session.

show idb

To display information about the status of interface descriptor blocks (IDBs), use the **show idb** command in privileged EXEC mode.

show idb

Syntax Description

This command has nor arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1	This command was introduced.
12.2(15)T	The output of this command was changed to show additional information.

Examples

The following is sample output from the **show idb** command:

```
Router# show idb

Maximum number of Software IDBs 8192.  In use 17.

                        HWIDBs     SWIDBs
Active                       5         14
Inactive                    10          3
Total IDBs                  15         17
Size each (bytes)         5784       2576
Total bytes              86760      43792

HWIDB#1   1   2   GigabitEthernet0/0 0 5, HW IFINDEX, Ether)
HWIDB#2   2   3   GigabitEthernet9/0 0 5, HW IFINDEX, Ether)
HWIDB#3   3   4   GigabitEthernet9/1 6 5, HW IFINDEX, Ether)
HWIDB#4   4   5   GigabitEthernet9/2 6 5, HW IFINDEX, Ether)
HWIDB#5   13  1   Ethernet0 4 5, HW IFINDEX, Ether)
```

Table 72 describes the significant fields shown in the display.

Table 72 show idb Field Descriptions

Field	Description
In use	Total number of software IDBs (SWIDBs) that have been allocated. This number never decreases. SWIDBs are never deallocated.
Active	Total number of hardware IDBs (HWIDBs) and SWIDBs that are allocated and in use.
Inactive	Total number of HWIDBs and SWIDBs that are allocated but not in use.
Total	Total number of HWIDBs and SWIDBs that are allocated.

show ip director default

To verify default metric configuration information for DistributedDirector metrics, use the **show ip director default** command in privileged EXEC mode.

show ip director default [**priority** | **weight**]

Syntax Description

priority	(Optional) Default priorities for metrics
weight	(Optional) Default weights for metrics

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

Use this command to verify default metric configurations.

Examples

The following is sample output from the **show ip director default priority** command:

```
Router# show ip director default priority

Director default metric priorities:
random priority = 2
DRP route lookup external to AS priority = 1
administrative preference priority = 0
DRP route lookup internal to AS priority = 0
DRP distance to associated server priority = 0
portion priority = 0
Round-trip time from DRP to client priority = 0
DFP originated weight priority = 0
Route-map evaluation priority = 0
```

Related Commands

Command	Description
ip director default priorities	Sets default priorities for DistributedDirector metrics.

show ip director dfp

To display information about the current status of the DistributedDirector connections with a particular Dynamic Feedback Protocol (DFP) agent, use the **show ip director dfp** command in EXEC mode.

show ip director dfp [*host-name* | *ip-address*]

Syntax Description

host-name	(Optional) Host name.
ip-address	(Optional) IP address.

Command Modes

EXEC

Command History

Release	Modification
12.1(5)T	This command was introduced.

Examples

The following is sample output from the **show ip director dfp** command:

```
Router# show ip director dfp

172.24.9.9:
Max retries: 5
Timeout between connect attempts: 60
Timeout between updates: 90
Last update received: 00:00:12 ago
Server  Port BindID Address Mask
172.28.9.9 80 0  0.0.0.0 0.0.0.0
192.168.25.25
Max retries: 5
Timeout between connect attempts: 60
Timeout between updates: 90
Last update received: 00:00:44 ago
Server Port BindIDAddress Mask
192.168.30.30 800 0.0.0.0 0.0.0.0
```

show ip drp boomerang

To display the status of various boomerang domains, use the **show ip drp boomerang** command in privileged EXEC mode.

show ip drp boomerang [*domain-name*]

Syntax Description

domain-name	(Optional) Specified domain name.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

The **show ip drp boomerang** command can be used on the boomerang client to display the status of the various boomerang domains. The following information can be shown for each domain:

- Alias information—The number of DNS requests for each alias.
- Content server address information:
  - Number of DNS requests.
  - Number of requests dropped because server is down.
  - Number of requests dropped because there is no original server.
  - Number of requests dropped because of security failures.

Examples

The following is sample output from the **show ip drp boomerang** command:

```
Router# show ip drp boomerang www.boom1.com

DNS packets with unknown domain 0

  Domain www.boom1.com
    Content server            172.16.101.101 up
    Origin server                    0.0.0.0
    DNS A record requests                  0
    Dropped (server down)                  0
    Dropped (no origen server)             0
    Security failures                      0

  Alias www.boom2.com
    DNS A record requests                  0
```

Related Commands

Command	Description
alias (boomerang configuration)	Configures an alias name for a specified domain.
ip drp domain	Adds a new domain to the DistributedDirector client or configures an existing domain and puts the client in boomerang configuration mode.
server (boomerang configuration)	Configures the server address for a specified boomerang domain.
show ip drp	Displays DRP statistics on DistributedDirector or a DRP server agent.
ttl dns	Configures the number of seconds for which an answer received from the boomerang client will be cached by the DNS client.
ttl ip	Configures the IP TTL value for the boomerang response packets sent from the boomerang client to the DNS client in number of hops.

show ip http server

To display details about the current configuration of the HTTP server, use the **show ip http server** command in user EXEC or privileged EXEC mode.

show ip http server {**all** | **status** | **session-module** | **connection** | **statistics** | **history**}

Syntax Description

all	Displays all HTTP server information.
status	Displays only HTTP server status configuration.
session-module	Displays only supported HTTP services (Cisco IOS modules).
connection	Displays only the current connections to the HTTP server, including the local and remote IP addresses being accessed.
statistics	Displays only HTTP server connection statistics.
history	Displays only the previous 20 connections to the HTTP server, including the IP address accessed, and the time when the connection was closed.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use this command to show detailed status information about the HTTP server.

If the HTTP secure server capability is present, the output of the **show ip http server all** command will also include the information found in the output of the **show ip http server secure status** command.

Examples

The following is sample output from the **show ip http server all** command:

```
Router# show ip http server all

HTTP server status: Enabled
HTTP server port: 80
HTTP server authentication method: enable
HTTP server access class: 0
HTTP server base path:
Maximum number of concurrent server connections allowed: 5
Server idle time-out: 30 seconds
Server life time-out: 120 seconds
Maximum number of requests allowed on a connection: 2
HTTP secure server capability: Not Present
HTTP server application session modules:
 Session module Name  Handle  Description
Homepage_Server       5       IOS Homepage Server
QDM                   2       QOS Device Manager Server
HTTP IFS Server       1       HTTP based IOS File Server
QDM SA                3       QOS Device Manager Signed Applet Server
```

```
WEB_EXEC              4       HTTP based IOS EXEC Server
XSM                   6       XML Session Manager
VDM                   7       VPN Device Manager Server
ITS                   8       IOS Telephony Service
ITS_LOCDIR            9       ITS Local Directory Search

HTTP server current connections:
local-ipaddress:port   remote-ipaddress:port in-bytes  out-bytes
  172.19.254.37:80     128.190.254.45:33737  70        2294

HTTP server statistics:
Accepted connections total: 1360

HTTP server history:
local-ipaddress:port  remote-ipaddress:port  in-bytes  out-bytes  end-time
  172.91.254.37:80     128.190.254.45:63530  60        1596       10:50:00 12/19
```

Table 73 describes the significant fields shown in the display.

Table 73 show ip http server Field Descriptions

Field	Description
HTTP server status:	Enabled or disabled. Corresponds to the [**no**] **ip http server** command.
HTTP server port:	Port used by the HTTP server. Corresponds to the **ip http port** command.
HTTP server authentication method:	Authentication method used for HTTP server logins. Corresponds to the **ip http authentication** command.
HTTP server access class:	Access list number assigned to the HTTP server. A value of zero (0) indicates no access list is assigned. Corresponds to the **ip http access-class** command.
HTTP server base path:	Base HTTP path specifying the location of the HTTP server files (HTML files). Corresponds to the **ip http path** command.
Maximum number of concurrent server connections allowed:	Corresponds to the **ip http max-connections** command.
Server idle time-out:	The maximum number of seconds the connection will be kept open if no data is received or if response data can not be sent out. Corresponds to the **ip http timeout-policy** command.
Server life time-out:	The maximum number of seconds the connection will be kept open. Corresponds to the **ip http timeout-policy** command.
Maximum number of requests allowed on a connection:	The maximum number of requests that will be processed on a connection before the connection is closed. Corresponds to the **ip http timeout-policy** command.
HTTP secure server capability:	Indicates if the running software image supports the secure HTTP server (“Present” or “Not Present”). If the capability is present, the output from the **show ip http server secure status** command will appear after this line.

Table 73 show ip http server Field Descriptions (continued)

Field	Description
HTTP server application session modules:	Cisco IOS services that use the HTTP server. Services are provided for application interfaces, including: • the Cisco Web browser user interface, which uses the Cisco IOS Homepage Server, HTTP-based EXEC Server, and HTTP IOS File System (IFS) Server • the VPN Device Manager (VDM) application, which uses the VDM Server and the XML Session Manager (XSM) • the QoS Device Manager (QDM) application, which uses the QDM Server • the IP Phone and Cisco IOS Telephony Service applications, which use the ITS Local Directory Search and IOS Telephony Server (ITS)
HTTP server current connections:	Currently active HTTP connections.
HTTP server statistics:	How many connections have been accepted.
HTTP server history:	Details about the last 20 connections, including the time the connection was closed (end-time). End-time is given in Universal Coordinated Time (UTC or GMT), using a 24-hour clock and the following format: *hh*:*mm*:*ss month*/*day*

The following example shows sample output for the **show ip http server status** command:

```
Router# show ip http server status
HTTP server status: Disabled
HTTP server port: 80
HTTP server authentication method: enable
HTTP server access class: 0
HTTP server base path:
Maximum number of concurrent server connections allowed: 5
Server idle time-out: 600 seconds
Server life time-out: 600 seconds
Maximum number of requests allowed on a connection: 1
HTTP secure server capability: Present
HTTP secure server status: Disabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-12a
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint:
```

The lines indicating the status of the HTTP secure (HTTPS) server will only be visible if your software image supports the HTTPS server. If your software image does not support SSL, only the following line will be visible:

HTTP secure server capability: Not present

Related Commands

Command	Description
debug ip http server all	Enables debugging output for all HTTP processes on the system.
ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface.
ip http secure-server	Enables the secure HTTP (HTTPS) server.
show ip http server secure status	Displays the status of the secure HTTP (HTTPS) server.

show kron schedule

To display the status and schedule information of Command Scheduler occurrences, use the **show kron schedule** command in user Exec or privileged Exec mode.

show kron schedule

Syntax Description

This command has no arguments or keywords.

Default

None

Command Mode

Exec

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use the **show kron schedule** command to view all currently configured occurrences and when they are next scheduled to run.

Examples

The following sample output displays each configured policy name and the time interval before the policy is scheduled to run:

```
Router# show kron schedule

Kron Occurrence Schedule
week inactive, will run again in 7 days 01:02:33
may inactive, will run once in 32 days 20:43:31 at 6:30 on Jun 20
```

Table 74 describes the significant fields shown in the display.

Table 74 show kron schedule Field Descriptions

Field	Description
week inactive	The policy list named week is currently inactive.
run again in 7 days 01:02:33	Time in days, hours, minutes and seconds before the policy will run. This policy is scheduled to run on a recurring basis.
run once in 32 days 20:434:31	Time in days, hours, minutes and seconds before the policy will run. This policy is scheduled to run just once.

Related Commands

Command	Description
kron occurrence	Specifies schedule parameters for a Command Scheduler occurrence and enters kron-occurrence configuration mode.
policy-list	Specifies the policy list associated with a Command Scheduler occurrence.

show logging

To display the state of system logging (syslog) and the contents of the standard system logging message buffer, use the **show logging** command in privileged Exec mode.

show logging [**slot** *slot-number* | **summary**]

Syntax Description

slot *slot-number*	(Optional) Displays information in the syslog history table for a specific line card. Slot numbers range from 0 to 11 for the Cisco 12012 Internet router and 0 to 7 for the Cisco 12008 Internet router.
summary	(Optional) Displays counts of messages by type for each line card.

Default

None

Command Mode

Priviledged Exec

Command History

Release	Modification
10.0	This command was introduced.
11.2 GS	The **slot** and **summary** keywords were added for the Cisco 12000 family.
12.2(8)T	Command output was expanded to show the status of the logging count facility (“Count and timestamp logging messages”).
12.2(15)T	Command output was expanded to show the status of XML syslog formatting.

Usage Guidelines

This command displays the state of syslog error and event logging, including host addresses, and which logging destinations (console, monitor, buffer, or host) logging is enabled. This command also displays Simple Network Management Protocol (SNMP) logging configuration parameters and protocol activity.

This command will also display the contents of the standard system logging buffer, if logging to the buffer is enabled. Logging to the buffer is enabled or disabled using the [**no**] **logging buffered** command. The number of system error and debugging messages in the system logging buffer is determined by the configured size of the syslog buffer. This size of the syslog buffer is also set using the **logging buffered** command.

To enable and set the format for syslog message timestamping, use the **service timestamps log** command.

If debugging is enabled (using any **debug** command), and the logging buffer is configured to include level 7 (debugging) messages, debug output will be included in the system log. Debugging output is not formatted like system logging messages, and will not be preceeded by the percent symbol (%).

Examples

The following is sample output from the **show logging** command. In this example, buffer logging is disabled, so no syslog messages are displayed with this command.

```
Router# show logging

Syslog logging: enabled (0 messages dropped, 1 messages rate-limited, 0 flushes)
     Console logging: level debugging, 31 messages logged, xml disabled
     Monitor logging: level debugging, 0 messages logged, xml disabled
     Buffer logging: disabled, xml disabled
     Logging Exception size (4096 bytes)
     Count and timestamp logging messages: enabled
     Trap logging: level informational, 35 message lines logged
```

Table 75 describes the significant fields shown in the display.

Table 75 show logging Field Descriptions

Field	Description
Syslog logging	Shows general state of system logging (enabled or disabled), and status of logged messages (number of messages dropped, rate-limited, or flushed).
Console logging	Logging to the console port. Shows “disabled” or, if enabled, the severity level limit and number of messages logged. Enabled using the **logging console** command.
Monitor logging	Logging to the monitor (all TTY lines). Shows “disabled” or, if enabled, the severity level limit and number of messages logged. Enabled using the **logging monitor** command.
Buffer logging	Logging to the standard syslog buffer. Shows “disabled” or, if enabled, the severity level limit and number of messages logged. Enabled using the **logging buffered** command.
Trap logging	Logging to a remote host (syslog host). Shows “disabled” or, if enabled, the severity level limit and number of messages logged. (The word “trap” means a trigger in the system software for sending error messages to a remote host.) Prior to Cisco IOS release 12.2(15)T, trap logging was enabled using the **logging** <*host-name*> command. Now enabled using the **logging host** command. The severity level limit is set using the **logging trap** command.
SNMP logging	Displays whether SNMP logging is enabled, the number of messages logged, and the retransmission interval. If not shown on your platform, use the **show logging history** command.

The following example includes syslog messages from the system buffer, with timestamping :

```
Router> show logging

Syslog logging:enabled (2 messages dropped, 0 flushes, 0 overruns)
    Console logging:disabled
    Monitor logging:level debugging, 0 messages logged
    Buffer logging:level debugging, 4104 messages logged
    Trap logging:level debugging, 4119 message lines logged
        Logging to 216.231.111.14, 4119 message lines logged
Log Buffer (262144 bytes):

Jul 11 12:17:49 EDT:%BGP-4-MAXPFX:No. of prefix received from 209.165.200.225 (afi 0)
reaches 24, max 24
```

```
! THE FOLLOWING LINE IS A DEBUG MESSAGE FROM NTP.
! NOTE THAT IT IS NOT PRECEEDED BY THE % SYMBOL.
Jul 11 12:17:48 EDT: NTP: Maxslew = 213866
Jul 11 15:15:41 EDT:%SYS-5-CONFIG:Configured from tftp://host.com/addc5505-rsm.nyiix
.Jul 11 15:30:28 EDT:%BGP-5-ADJCHANGE:neighbor 209.165.200.226 Up
.Jul 11 15:31:34 EDT:%BGP-3-MAXPFXEXCEED:No. of prefix received from
209.165.200.226 (afi 0):16444 exceed limit 375
.Jul 11 15:31:34 EDT:%BGP-5-ADJCHANGE:neighbor 209.165.200.226 Down BGP
Notification sent
.Jul 11 15:31:34 EDT:%BGP-3-NOTIFICATION:sent to neighbor 209.165.200.226 3/1 (update
malformed) 0 bytes
. . .
```

The software clock keeps an "authoritative" flag that indicates whether the time is authoritative (believed to be accurate). If the software clock has been set by a timing source (for example, via NTP), the flag is set. If the time is not authoritative, it will be used only for display purposes. Until the clock is authoritative and the "authoritative" flag is set, the flag prevents peers from synchronizing to the software clock.

Table 76 decribes the symbols that proceed the timestamp.

Table 76 Timestamping Symbols for syslog Messages

Symbol	Description	Example
*	Time is not authoritative: the software clock is not in sync or has never been set.	*15:29:03.158 UTC Tue Feb 25 2003:
(blank)	Time is authoritative: the software clock is in sync or has just been set manually	15:29:03.158 UTC Tue Feb 25 2003:
.	Time is authoritative, but NTP is not synchronized: the software clock was in sync, but has since lost contact with all configured NTP servers	.15:29:03.158 UTC Tue Feb 25 2003:

The following is sample output from the **show logging summary** command for a Cisco 12012 router. A number in the column indicates that the syslog contains that many messages for the line card. For example, line card in slot 9 has 1 error message, 4 warning messages, and 47 notification messages.

Note For similar log counting on other platforms, use the **show logging count** command.

```
Router# show logging summary

+-----+-------+-------+-------+-------+-------+-------+-------+-------+
 SLOT | EMERG | ALERT | CRIT  | ERROR |WARNING| NOTICE| INFO  | DEBUG |
+-----+-------+-------+-------+-------+-------+-------+-------+-------+
|* 0* |     . |     . |     . |     . |     . |     . |     . |     . |
|  1  |       |       |       |       |       |       |       |       |
|  2  |       |       |       |     1 |     4 |    45 |       |       |
|  3  |       |       |       |       |       |       |       |       |
|  4  |       |       |       |     5 |     4 |    54 |       |       |
|  5  |       |       |       |       |       |       |       |       |
|  6  |       |       |       |       |       |       |       |       |
|  7  |       |       |       |    17 |     4 |    48 |       |       |
|  8  |       |       |       |       |       |       |       |       |
|  9  |       |       |       |     1 |     4 |    47 |       |       |
| 10  |       |       |       |       |       |       |       |       |
| 11  |       |       |       |    12 |     4 |    65 |       |       |
+-----+-------+-------+-------+-------+-------+-------+-------+-------+
```

```
Router#
```

Table 77 describes the logging level fields shown in the display.

Table 77 show logging summary Field Descriptions

Field	Description
SLOT	Indicates the slot number of the line card. An asterisk next to the slot number indicates the GRP card whose error message counts are not displayed. For information on the GRP card, use the **show logging** command.
EMERG	Indicates that the system is unusable.
ALERT	Indicates that immediate action is needed.
CRIT	Indicates a critical condition.
ERROR	Indicates an error condition.
WARNING	Indicates a warning condition.
NOTICE	Indicates a normal but significant condition.
INFO	Indicates an informational message only.
DEBUG	Indicates a debugging message.

Related Commands

Command	Description
clear logging	Clears messages from the logging buffer.
logging count	Enables the error log count capability.
logging history size	Changes the number of syslog messages stored in the history table of the router.
logging linecard	Logs messages to an internal buffer on a line card and limits the logging messages displayed on terminal lines other than the console line to messages with a level at or above level.
service timestamps	Configures the system to timestamp debugging or logging messages.
show logging count	Displays a summary of system error messages (syslog messages) by facility and severity.
show logging xml	Displays the state of system logging and the contents of the XML-specific logging buffer.

show logging count

To display a summary of the number of times certain system error messages are occuring, use the **show logging** command in privileged Exec mode.

show logging count

Syntax Description

This command has no arguements or keywords.

Command Mode

Privileged Exec

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

To enable the error log count capability (syslog counting feature), use the **logging count** command in global configuration mode.

This feature works independently of the various settings of the other logging commands (such as [**no**] **logging on**, [**no**] **logging buffered**, and so on). In other words, turning off logging by other means does not stop the counting and timestamping from occuring.

This command displays information such as the number of times a particular system error message occurs and the time stamp of the last occurrence of the specified message. System error messages are grouped into logical units called "Facilities" based on Cisco IOS software components.

To determine if system error message counting is enabled, use the **show logging** command.

The **service timestamps** command configuration determines the timestamp format (shown in the "Last Time" column) of **show logging count** command output. There is not quite enough space for all options of the possible options (datetime, milliseconds, and timezone) of the **service timestamps datetime** command to be displayed at the same time. As a result, if **msec** is selected, **timezone** will not be displayed. If **show-timezone** is selected but not **msec**, then the time zone will be displayed.

Occasionally, the length of the message name plus the facility name contains too many characters to be printed on one line. The CLI attempts to keep the name and facility name on one line but, if necessary, the line will be wrapped, so that the first line contains the facility name and the second line contains the message name and the rest of the columns.

Examples

The following example shows the number of times syslog messages have occurred and the most recent time that each error message occurred. In this example, the **show logging** command is used to determine if the syslog counting feature is enabled:

```
Router# show logging | include count
Count and timestamp logging messages: enabled
```

```
Router# show logging count

Facility       Message Name                      Sev  Occur  Last Time
================================================================================
SYS            BOOTTIME                            6    1   00:00:12
SYS            RESTART                             5    1   00:00:11
SYS            CONFIG_I                            5    1   00:00:05
-------------  -------------------------------  ------------------------------
SYS TOTAL                                              3

LINEPROTO      UPDOWN                              5   13   00:00:19
-------------  -------------------------------  ------------------------------
LINEPROTO TOTAL                                       13

LINK           UPDOWN                              3    1   00:00:18
LINK           CHANGED                             5   12   00:00:09
-------------  -------------------------------  ------------------------------
LINK TOTAL                                            13

SNMP           COLDSTART                           5    1   00:00:11
-------------  -------------------------------  ------------------------------
SNMP TOTAL                                             1
```

Table 78 describes the significant fields shown in the display.

Table 78 show logging count Field Descriptions

Field	Description
Facility	The facility, such as syslog, from which these error messages are occurring.
Message Name	The name of this message.
Sev	The severity level of this message.
Occur	How many times this message has occurred.
Last Time	The last (most recent) time this message occurred. Timestamping is by default based on the system uptime (for example “3w1d” indicates 3 weeks and 1 day from the last system reboot.)
Sys Total / Lineproto Total / Link Total / SNMP Total	Total number of error messages that have occurred for the specified Facility.

In the following example, the user is interested only in the totals:

```
Router# show logging count | include total
SYS TOTAL                                              3
LINEPROTO TOTAL                                       13
LINK TOTAL                                            13
SNMP TOTAL                                             1
```

Related Commands

Command	Description
clear logging	Clears messages from the logging buffer.
logging count	Enables the system error message log count capability.
service timestamps	Configures the system to time-stamp debugging or logging messages.
show logging	Displays general information about the state of system logging.

show logging history

To display information about the state of the syslog history table, use the **show logging history** command in privileged Exec mode.

show logging history

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged Exec

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command displays information about the syslog history table, such as the table size, the status of messages, and text of messages stored in the table. Messages stored in the table are governed by the **logging history** global configuration command.

Examples

The following example shows sample output from the **show logging history** command. In this example, notifications of severity level 5 (notifications) through severity level 0 (emergencies) are configured to be written to the logging history table.

```
Router# show logging history

Syslog History Table: 1 maximum table entries,
saving level notifications or higher
0 messages ignored, 0 dropped, 15 table entries flushed,
SNMP notifications not enabled
  entry number 16: SYS-5-CONFIG_I
  Configured from console by console
  timestamp: 1110
Router#
```

Table 79 describes the significant fields shown in the output.

Table 79 show logging history Field Descriptions

Field	Description
maximum table entry	Number of messages that can be stored in the history table. Set with the **logging history size** command.
saving level notifications <x> or higher	Level of messages that are stored in the history table and sent to the SNMP server (if SNMP notification is enabled). The severity level can be configured with the **logging history** command.

Table 79 show logging history Field Descriptions (continued)

Field	Description
messages ignored	Number of messages not stored in the history table because the severity level is greater than that specified with the **logging history** command.
dropped	Number of messages that could not be processed due to lack of system resources. Dropped messages do not appear in the history table and are not sent to the SNMP server.
table entries flushed	Number of messages that have been removed from the history table to make room for newer messages.
SNMP notifications	Whether syslog traps of the appropriate level are sent to the SNMP server. The sending of syslog traps are enabled or disabled through the **snmp-server enable traps syslog** command.
entry number:	Number of the message entry in the history table. In the example above, the message "SYS-5-CONFIG_I Configured from console by console" indicates a syslog message consisting of the facility name (SYS), which indicates where the message came from, the severity level (5) of the message, the message name (CONFIG_I), and the message text.
timestamp	Time, based on the up time of the router, that the message was generated.

Related Commands

Command	Description
clear logging	Clears messages from the logging buffer.
logging history	Limits syslog messages sent to the router's history table to a specified severity level.
logging history size	Changes the number of syslog messages that can be stored in the history table.
logging linecard	Logs messages to an internal buffer on a line card. This command limits the logging messages displayed on terminal lines other than the console line to messages with a level at or above level.
snmp-server enable traps	The [**no**] **snmp-server enable traps syslog** form of this command controls (enables or disables) the sending of system-logging messages to a network management station.

show logging xml

To display the state of system message logging in an XML format, and to display the contents of the XML syslog buffer, use the **show logging xml** command in privileged Exec mode.

show logging xml

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged Exec

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

This command displays the same syslog state information as the standard **show logging** command, but displays the information in XML format. This command also displays the content of the XML syslog buffer (if XML-formatted buffer logging is enabled).

Examples

The following example compares the output of the standard **show logging** command with the output of the **show logging xml** command so that you can see how the standard information is formatted in XML.

```
Router# show logging

Syslog logging: enabled (10 messages dropped, 6 messages rate-limited, 0 flushes, 0
overruns, xml enabled)
    Console logging: level debugging, 28 messages logged, xml enabled
    Monitor logging: level debugging, 0 messages logged, xml enabled
    Buffer logging: level debugging, 2 messages logged, xml enabled (2 messages logged)
    Logging Exception size (8192 bytes)
    Count and timestamp logging messages: disabled
    Trap logging: level informational, 35 message lines logged
        Logging to 1.2.3.4, 1 message lines logged, xml disabled
        Logging to 4.3.2.1, 1 message lines logged, xml enabled

Log Buffer (8192 bytes):

00:04:20: %SYS-5-CONFIG_I: Configured from console by console
00:04:41: %SYS-5-CONFIG_I: Configured from console by console

Router# show logging xml

<syslog-logging status="enabled" msg-dropped="10" msg-rate-limited="6" flushes="0"
overruns="0"><xml>enabled</xml></syslog-logging>
    <console-logging level="debugging"
messages-logged="28"><xml>enabled</xml></console-logging>
    <monitor-logging level="debugging"
messages-logged="0"><xml>enabled</xml></monitor-logging>
    <buffer-logging level="debugging" messages-logged="2"><xml
messages-logged="2">enabled</xml></buffer-logging>
    <logging-exception size="8192 bytes"></logging-exception>
```

```
    <count-and-timestamp-logging status="disabled"></count-and-timestamp-logging>
    <trap-logging level="informational" messages-lines-logged="35"></trap-logging>
        <logging-to><dest id="0" ipaddr="1.2.3.4"
message-lines-logged="1"><xml>disabled</xml><dest></logging-to>
        <logging-to><dest id="1" ipaddr="4.3.2.1"
message-lines-logged="1"><xml>enabled</xml><dest></logging-to>

<log-xml-buffer size="44444 bytes"></log-xml-buffer>

<ios-log-msg><facility>SYS</facility><severity>5</severity><msg-id>CONFIG_I</msg-id><time>
00:04:20</time><args><arg id="0">console</arg><arg
id="1">console</arg></args></ios-log-msg>
<ios-log-msg><facility>SYS</facility><severity>5</severity><msg-id>CONFIG_I</msg-id><time>
00:04:41</time><args><arg id="0">console</arg><arg
id="1">console</arg></args></ios-log-msg>
Router#
```

Table 80 describes the significant fields shown in the displays.

Table 80 show logging and show logging xml Field Descriptions

Field	Description	XML Tag
Syslog logging	The global state of system message logging (syslog); “enabled” or “disabled.”	syslog-logging
Console logging	State of logging to console connections.	console-logging
Monitor logging	State of logging to monitor (TTY and Telnet) connections.	monitor-logging
Buffer logging	State of logging to the local system logging buffer.	buffer-logging
Count and timestamp logging messages:	Indicates whether the logging count feature is enabled. Corresponds to the **logging count** command.	count-and-timestamp-logging
Trap logging	State of logging to a remote host.	trap-logging

Related Commands

Command	Description
show logging count	Displays counts of each system error message.
show logging history	Displays the contents of the SNMP syslog history table.
show logging	Displays the contents of the standard syslog buffer.

show management event

To display the Simple Network Management Protocol (SNMP) Event values that have been configured on your routing device through the use of the Event MIB, use the **show management event** command in privileged Exec mode.

show management event

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged Exec

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

The Event MIB allows you to configure your own traps, informs, or set operations through the use of an external network management application. The **show management event** command is used to display the values for the Events configured on your system. There are no Cisco IOS CLI commands for configuring Event MIB values. For information on Event MIB functionality, see RFC 2981, available at http://www.ietf.org.

Examples

The following example shows sample output of the **show management event** command:

```
Router# show management event

Mgmt Triggers:
 (1): Owner: joe_user
  (1): 01, Comment: TestEvent, Sample: Abs, Freq: 120
      Test: Existence Threshold Boolean
         ObjectOwner: aseem, Object: sethi
         OID: ifEntry.10.3, Enabled 1, Row Status 1
      Existence Entry: , Absent, Changed
      StartUp:  Present, Absent
         ObjOwn: , Obj: , EveOwn: aseem, Eve: 09
      Boolean Entry:
         Value: 10, Cmp: 1, Start: 1
         ObjOwn: , Obj: , EveOwn: aseem, Eve: 09
      Threshold Entry:
         Rising: 50000, Falling: 20000
         ObjOwn: ase, Obj: 01 RisEveOwn: ase, RisEve: 09 , FallEveOwn: ase, FallEve: 09

      Delta Value Table:
  (0): Thresh: Rising, Exis: 1, Read: 0, OID: ifEntry.10.3 , val: 69356097
```

```
Mgmt Events:
(1): Owner: aseem
  (1)Name: 09 , Comment: , Action: Set, Notify, Enabled: 1 Status: 1
     Notification Entry:
        ObjOwn: , Obj: , OID: ifEntry.10.1
     Set:
        OID: ciscoSyslogMIB.1.2.1.0, SetValue: 199, Wildcard: 2 TAG: , ContextName:

Object Table:
(1): Owner: aseem
  (1)Name: sethi, Index: 1, OID: ifEntry.10.1, Wild: 1, Status: 1
```

Related Commands

Command	Description
debug management event	Allows real-time monitoring of Event MIB activities for the purposes of debugging.

show memory

To show statistics about memory, including memory-free pool statistics, use the **show memory** command in Exec mode.

show memory [*address*] [*memory-type*] [**free**] [**summary**]

Syntax Description

address	Show memory details starting at the specified address. **Note** You can also use the standard **show** command extensions to filter the output, such as **show memory | begin** *address*.
memory-type	(Optional) Memory type to display. If *memory-type* is not specified, statistics for all memory types present are displayed. Memory types include: • **dead** • **free** • **io** • **multibus** • **overflow** • **pci** • **processor** • **statistics** (memory pool statistics)
free	(Optional) Displays free memory statistics.
summary	(Optional) Displays a summary of memory usage including the size and number of blocks allocated for each address of the system call that allocated the block.

Command Mode

Exec

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **show memory** command displays information about memory available after the system image decompresses and loads.

Examples

The following is sample output from the **show memory** command:

```
Router# show memory

              Head   Total(b)    Used(b)    Free(b)  Lowest(b) Largest(b)
Processor    B0EE38    5181896    2210036    2971860    2692456    2845368

          Processor memory
Address   Bytes Prev.    Next     Ref  PrevF   NextF   Alloc PC  What
B0EE38     1056 0        B0F280     1                  18F132    List Elements
```

```
B0F280     2656 B0EE38   B0FD08     1                 18F132    List Headers
B0FD08     2520 B0F280   B10708     1                 141384    TTY data
B10708     2000 B0FD08   B10F00     1                 14353C    TTY Input Buf
B10F00      512 B10708   B11128     1                 14356C    TTY Output Buf
B11128     2000 B10F00   B11920     1                 1A110E    Interrupt Stack
B11920       44 B11128   B11974     1                 970DE8    *Init*
B11974     1056 B11920   B11DBC     1                 18F132    messages
B11DBC       84 B11974   B11E38     1                 19ABCE    Watched Boolean
B11E38       84 B11DBC   B11EB4     1                 19ABCE    Watched Boolean
B11EB4       84 B11E38   B11F30     1                 19ABCE    Watched Boolean
B11F30       84 B11EB4   B11FAC     1                 19ABCE    Watched Boolean
Router#
```

The following is sample output from the **show memory free** command:

```
Router# show memory free

               Head   Total(b)    Used(b)    Free(b)  Lowest(b) Largest(b)
Processor      B0EE38    5181896    2210076    2971820    2692456    2845368

          Processor memory
Address   Bytes Prev.    Next     Ref  PrevF   NextF   Alloc PC  What
             24    Free list 1
CEB844       32  CEB7A4 CEB88C      0  0       0       96B894    SSE Manager
             52    Free list 2
             72    Free list 3
             76    Free list 4
             80    Free list 5
D35ED4       80 D35E30   D35F4C     0  0       D27AE8  96B894    SSE Manager
D27AE8       80 D27A48   D27B60     0  D35ED4  0       22585E    SSE Manager
             88    Free list 6
            100    Free list 7
D0A8F4      100 D0A8B0   D0A980     0  0       0       2258DA    SSE Manager
            104    Free list 8
B59EF0      108 B59E8C   B59F84     0  0       0       2258DA    (fragment)
```

The output of the **show memory free** command contains the same types of information as the **show memory** output, except that only free memory is displayed, and the information is displayed in order for each free list.

The first section of the display includes summary statistics about the activities of the system memory allocator. Table 81 describes the significant fields shown in the first section of the display.

Table 81 show memory Field Descriptions—First Section

Field	Description
Head	Hexadecimal address of the head of the memory allocation chain.
Total(b)	Sum of used bytes plus free bytes.
Used(b)	Amount of memory in use.
Free(b)	Amount of memory not in use.
Lowest(b)	Smallest amount of free memory since last boot.
Largest(b)	Size of largest available free block.

The second section of the display is a block-by-block listing of memory use. Table 82 describes the significant fields shown in the second section of the display.

Table 82 Characteristics of Each Block of Memory—Second Section

Field	Description
Address	Hexadecimal address of block.
Bytes	Size of block (in bytes).
Prev.	Address of previous block (should match Address on previous line).
Next	Address of next block (should match address on next line).
Ref	Reference count for that memory block, indicating how many different processes are using that block of memory.
PrevF	Address of previous free block (if free).
NextF	Address of next free block (if free).
Alloc PC	Address of the system call that allocated the block.
What	Name of process that owns the block, or "(fragment)" if the block is a fragment, or "(coalesced)" if the block was coalesced from adjacent free blocks.

The **show memory io** command displays the free I/O memory blocks. On the Cisco 4000 router, this command quickly shows how much unused I/O memory is available.

The following is sample output from the **show memory io** command:

```
Router# show memory io

Address   Bytes Prev.   Next     Ref  PrevF   NextF   Alloc PC  What
6132DA0   59264 6132664 6141520  0    0       600DDEC  3FCF0     *Packet Buffer*
600DDEC     500 600DA4C 600DFE0  0   6132DA0 600FE68  0
600FE68     376 600FAC8 600FFE0  0   600DDEC 6011D54  0
6011D54     652 60119B4 6011FEO  0   600FE68 6013D54  0
614FCA0     832 614F564 614FFE0  0   601FD54 6177640  0
6177640 2657056 6172E90 0        0   614FCA0 0        0
Total: 2723244
```

The **show memory summary** command displays a summary of all memory pools and memory usage per Alloc PC (address of the system call that allocated the block).

The following is a partial sample output from the **show memory summary** command. This command shows the size, blocks, and bytes allocated. Bytes equal the size multiplied by the blocks. For a description of the other fields, see Table 20 and Table 21.

```
Router# show memory summary

Head   Total(b)    Used(b)    Free(b)  Lowest(b) Largest(b)
Processor    B0EE38    5181896    2210216    2971680    2692456    2845368

          Processor memory
Alloc PC        Size     Blocks      Bytes    What
0x2AB2           192          1        192    IDB: Serial Info
0x70EC            92          2        184    Init
0xC916           128         50       6400    RIF Cache
0x76ADE         4500          1       4500    XDI data
0x76E84         4464          1       4464    XDI data
0x76EAC          692          1        692    XDI data
0x77764          408          1        408    Init
0x77776          116          1        116    Init
0x777A2          408          1        408    Init
0x777B2          116          1        116    Init
0xA4600           24          3         72    List
```

```
0xD9B5C           52          1         52    SSE Manager
.....................
0x0                0       3413    2072576    Pool Summary
0x0                0         28    2971680    Pool Summary (Free Blocks)
0x0               40       3441     137640    Pool Summary(All Block Headers)
0x0                0       3413    2072576    Memory Summary
0x0                0         28    2971680    Memory Summary (Free Blocks)
```

Related Commands

Command	Description
show memory fast	Displays fast (processor) memory statistics.
show processes memory	Displays memory used per process.

show memory fast

To display fast memory details for the router, use the **show memory fast** command.

show memory fast [**allocating-process** [**totals**] | **dead** [**totals**] | **free** [**totals**]]

Syntax Description

allocating-process	(Optional) Include allocating process names with the standard output.
dead	(Optional) Display only memory owned by dead processes.
free	(Optional) Display only memory not allocated to a process.
totals	(Optional) Summarizes the statistics for allocating processes, dead memory, or free memory.

Command Modes

Exec

Command History

Release	Modification
12.1	This command was introduced in a release prior to 12.1. This command replaced the **show memory sram** command.

Usage Guidelines

The show memory fast command displays the statistics for the fast memory. “Fast memory” is another name for “processor memory,” and is also known as “cache memory.” Cache memory is called fast memory because the processor can generally access the local cache (traditionally stored on SRAM positioned close to the processor) much more quickly than main memory or RAM.

Note The **show memory fast** command is a command alias for the **show memory processor** command. These commands will issue the same output.

Examples

The following example shows sample output from the **show memory fast** and the **show memory processor** commands:

```
Router>show memory fast

          Processor memory

 Address      Bytes     Prev     Next Ref     PrevF    NextF Alloc PC  what
8404A580 0001493284 00000000 841B6ECC 000  0        84BADF88 815219D8  (coalesced)
841B6ECC 0000020004 8404A580 841BBD18 001  -------- -------- 815DB094  Managed Chunk Queue
Elements
841BBD18 0000001504 841B6ECC 841BC320 001  -------- -------- 8159EAC4  List Elements
841BC320 0000005004 841BBD18 841BD6D4 001  -------- -------- 8159EB04  List Headers
841BD6D4 0000000048 841BC320 841BD72C 001  -------- -------- 81F2A614  *Init*
841BD72C 0000001504 841BD6D4 841BDD34 001  -------- -------- 815A9514  messages
841BDD34 0000001504 841BD72C 841BE33C 001  -------- -------- 815A9540  Watched messages
841BE33C 0000001504 841BDD34 841BE944 001  -------- -------- 815A95E4  Watched Semaphore
841BE944 0000000504 841BE33C 841BEB64 001  -------- -------- 815A9630  Watched Message
Queue
```

```
841BEB64 0000001504 841BE944 841BF16C 001  -------- -------- 815A9658  Watcher Message
Queue
841BF16C 0000001036 841BEB64 841BF5A0 001  -------- -------- 815A2B24  Process Array
-- More --
<Ctrl+z>

Router>show memory processor

          Processor memory

 Address      Bytes     Prev     Next Ref     PrevF    NextF Alloc PC  what
8404A580 0001493284 00000000 841B6ECC 000  0        84BADF88 815219D8  (coalesced)
841B6ECC 0000020004 8404A580 841BBD18 001  -------- -------- 815DB094  Managed Chunk Queue
Elements
841BBD18 0000001504 841B6ECC 841BC320 001  -------- -------- 8159EAC4  List Elements
841BC320 0000005004 841BBD18 841BD6D4 001  -------- -------- 8159EB04  List Headers
841BD6D4 0000000048 841BC320 841BD72C 001  -------- -------- 81F2A614  *Init*
841BD72C 0000001504 841BD6D4 841BDD34 001  -------- -------- 815A9514  messages
841BDD34 0000001504 841BD72C 841BE33C 001  -------- -------- 815A9540  Watched messages
841BE33C 0000001504 841BDD34 841BE944 001  -------- -------- 815A95E4  Watched Semaphore
841BE944 0000000504 841BE33C 841BEB64 001  -------- -------- 815A9630  Watched Message
Queue
841BEB64 0000001504 841BE944 841BF16C 001  -------- -------- 815A9658  Watcher Message
Queue
841BF16C 0000001036 841BEB64 841BF5A0 001  -------- -------- 815A2B24  Process Array
-- More --
<Ctrl+z>

Router>
```

The following example shows sample output from the **show memory fast allocating-process** command, followed by sample output from the **show memory fast allocating-process totals** command:

```
Router#show memory fast allocating-process

          Processor memory

 Address      Bytes     Prev     Next Ref   Alloc Proc     Alloc PC  What
8404A580 0001493284 00000000 841B6ECC 000                  815219D8  (coalesced)
841B6ECC 0000020004 8404A580 841BBD18 001  *Init*          815DB094  Managed Chunk Queue
Elements
841BBD18 0000001504 841B6ECC 841BC320 001  *Init*          8159EAC4  List Elements
841BC320 0000005004 841BBD18 841BD6D4 001  *Init*          8159EB04  List Headers
841BD6D4 0000000048 841BC320 841BD72C 001  *Init*          81F2A614  *Init*
841BD72C 0000001504 841BD6D4 841BDD34 001  *Init*          815A9514  messages
841BDD34 0000001504 841BD72C 841BE33C 001  *Init*          815A9540  Watched messages
841BE33C 0000001504 841BDD34 841BE944 001  *Init*          815A95E4  Watched Semaphore
841BE944 0000000504 841BE33C 841BEB64 001  *Init*          815A9630  Watched Message Queue
841BEB64 0000001504 841BE944 841BF16C 001  *Init*          815A9658  Watcher Message Queue
841BF16C 0000001036 841BEB64 841BF5A0 001  *Init*          815A2B24  Process Array
 --More--
<Ctrl+z>

c2600-1#show memory fast allocating-process totals

Allocator PC Summary for: Processor

    PC          Total   Count  Name
0x815C085C    1194600     150  Process Stack
0x815B6C28     948680       5  pak subblock chunk
0x819F1DE4     524640       8  BGP (0) update
0x815C4FD4     393480       6  MallocLite
```

```
0x815B5FDC     351528      30  TW Buckets
0x819F14DC     327900       5  connected
0x81A1E838     327900       5  IPv4 Unicast net-chunk(8)
0x8153DFB8     248136     294  *Packet Header*
0x82142438     133192       4  CEF: 16 path chunk pool
0x82151E0C     131116       1  Init
0x819F1C8C     118480       4  BGP (0) attr
0x815A4858     100048     148  Process
0x8083DA44      97248      17


 --More--
<Ctrl+z>
```

The following example shows sample output from the **show memory fast dead** command:

```
Router#show memory fast dead

          Processor memory

 Address      Bytes     Prev     Next Ref     PrevF    NextF Alloc PC  what
8498FC20 0000000028 8498FB90 8498FC64 001  -------- -------- 81472B24  AAA MI SG NAME
        -------
             68
Router#show memory fast dead totals

Dead Proc Summary for: Processor

    PC          Total   Count  Name
0x81472B24         68       1  AAA MI SG NAME

Router#
```

show memory scan

To monitor the number and type of parity (memory) errors on your system, use the **show memory scan** command in Exec mode.

show memory scan

Syntax Description

This command has no arguments or keywords.

Default

None

Command Mode

Exec

Command History

Release	Modification
12.0(4)XE	This command was introduced for the Cisco 7500 series.
12.0(7)T	This command was implemented in Cisco IOS Release 12.0T for the Cisco 7500 series.
12.0(6)S	This command was implemented in Cisco IOS Release 12.0S for the Cisco 7500 series.
12.1(1)E	This command was implemented in Cisco IOS Release 12.1E for the Cisco 7500 series.

Usage Guidelines

For the show memory scan command to function, the memory scan feature must be enabled on the RSP using the **memory scan** global configuraiton mode command.

Examples

The following example shows a result with no memory errors:

```
Router# show memory scan

Memory scan is on.
No parity error has been detected.
```

If errors are detected in the system, the **show memory scan** command generates an error report. In the following example, memory scan detected a parity error:

```
Router# show memory scan

Memory scan is on.
Total Parity Errors 1.
Address   BlockPtr   BlckSize  Disposit  Region Timestamp
6115ABCD  60D5D090   9517A4    Scrubed   Local 16:57:09 UTC Thu  Mar 18
```

Table 83 describes the fields contained in the error report.

Table 83 show memory scan Field Descriptions

Field	Description
Address	The byte address where the error occurred.
BlockPtr	The pointer to the block that contains the error.
BlckSize	The size of the memory block
Disposit	The action taken in response to the error: • BlockInUse—An error was detected in a busy block. • InFieldPrev—An error was detected in the previous field of a block header. • InHeader—An error was detected in a block header. • Linked—A block was linked to a bad list. • MScrubed—The same address was "scrubbed" more than once, and the block was linked to a bad list. • MultiError—Multiple errors have been found in one block. • NoBlkHdr—No block header was found. • NotYet—An error was found; no action has been taken at this time. • Scrubed—An error was "scrubbed." • SplitLinked—A block was split, and only a small portion was linked to a bad list.
Region	The memory region in which the error was found: • IBSS—image BSS • IData—imagedata • IText—imagetext • local—heap
Timestamp	The time the error occurred.

show microcode

To display microcode image information available on line cards, use the **show microcode** command in Exec mode.

show microcode

Syntax Description

This command has no arguments or keywords.

Command Mode

Exec

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample output from the **show microcode** command:

```
Router# show microcode

Microcode bundled in system

Card    Microcode    Target Hardware    Description
Type    Version      Version
----    ---------    ---------------    -----------
SP         2.3            11.x          SP version 2.3
EIP        1.1             1.x          EIP version 1.1
TRIP       1.2             1.x          TRIP version 1.2
FIP        1.4             2.x          FIP version 1.4
HIP        1.1             1.x          HIP version 1.1
SIP        1.1             1.x          SIP version 1.1
FSIP       1.1             1.x          FSIP version 1.1
```

In the following example for the Cisco 7200 series router, the output from the **show microcode** command lists the hardware types that support microcode download. For each type, the default microcode image name is displayed. If there is a configured default override, that name also is displayed.

```
router# show microcode

Microcode images for downloadable hardware
HW Type             Microcode image names
-----------------------------------------
ecpa     default    slot0:xcpa26-0
         configured slot0:xcpa26-2
pcpa     default    slot0:xcpa26-4
```

Related Commands

Command	Description
microcode (7000/7500)	Specifies where microcode should be loaded from on Cisco 7500/7000RSP routers.
microcode (7200)	Configures a default override for the microcode that is downloaded to the hardware on a Cisco 7200 series router.

show ntp associations

To show the status of Network Time Protocol (NTP) associations, use the **show ntp associations** command in Exec mode.

show ntp associations [**detail**]

Syntax Description

detail	(Optional) Displays detailed information about each NTP association.

Command Mode

Exec

Command History

Release	Modification
10.0	This command was introduced.

Examples

Detailed descriptions of the information displayed by this command can be found in the NTP specification (RFC 1305).

The following is sample output from the **show ntp associations** command:

```
Router> show ntp associations

     address         ref clock     st  when  poll  reach  delay  offset    disp
 ~172.31.32.2      172.31.32.1       5    29  1024  377     4.2   -8.59     1.6
+~192.168.13.33    192.168.1.111     3    69   128  377     4.1    3.48     2.3
*~192.168.13.57    192.168.1.111     3    32   128  377     7.9   11.18     3.6
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

Table 84 describes the significant fields shown in the display.

Table 84 show ntp associations Field Descriptions

Field	Description
(leading characters in display lines)	The first characters in a display line can be one or more of the following characters: * —Synchronized to this peer # —Almost synchronized to this peer + —Peer selected for possible synchronization - —Peer is a candidate for selection ~ —Peer is statically configured
address	Address of peer.
ref clock	Address of reference clock of peer.
st	Stratum of peer.
when	Time since last NTP packet was received from peer.
poll	Polling interval (in seconds).

Table 84 show ntp associations Field Descriptions (continued)

Field	Description
reach	Peer reachability (bit string, in octal).
delay	Round-trip delay to peer (in milliseconds).
offset	Relative time of peer clock to local clock (in milliseconds).
disp	Dispersion

The following is sample output of the **show ntp associations detail** command:

```
Router> show ntp associations detail

172.31.32.2 configured, insane, invalid, stratum 5
ref ID 172.31.32.1, time AFE252C1.6DBDDFF2 (00:12:01.428 PDT Mon Jul 5 1993)
our mode active, peer mode active, our poll intvl 1024, peer poll intvl 64
root delay 137.77 msec, root disp 142.75, reach 376, sync dist 215.363
delay 4.23 msec, offset -8.587 msec, dispersion 1.62
precision 2**19, version 3
org time AFE252E2.3AC0E887 (00:12:34.229 PDT Mon Jul 5 1993)
rcv time AFE252E2.3D7E464D (00:12:34.240 PDT Mon Jul 5 1993)
xmt time AFE25301.6F83E753 (00:13:05.435 PDT Mon Jul 5 1993)
filtdelay =     4.23    4.14    2.41    5.95    2.37    2.33    4.26    4.33
filtoffset =   -8.59   -8.82   -9.91   -8.42  -10.51  -10.77  -10.13  -10.11
filterror =     0.50    1.48    2.46    3.43    4.41    5.39    6.36    7.34

192.168.13.33 configured, selected, sane, valid, stratum 3
ref ID 192.168.1.111, time AFE24F0E.14283000 (23:56:14.078 PDT Sun Jul 4 1993)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 83.72 msec, root disp 217.77, reach 377, sync dist 264.633
delay 4.07 msec, offset 3.483 msec, dispersion 2.33
precision 2**6, version 3
org time AFE252B9.713E9000 (00:11:53.442 PDT Mon Jul 5 1993)
rcv time AFE252B9.7124E14A (00:11:53.441 PDT Mon Jul 5 1993)
xmt time AFE252B9.6F625195 (00:11:53.435 PDT Mon Jul 5 1993)
filtdelay =     6.47    4.07    3.94    3.86    7.31    7.20    9.52    8.71
filtoffset =    3.63    3.48    3.06    2.82    4.51    4.57    4.28    4.59
filterror =     0.00    1.95    3.91    4.88    5.84    6.82    7.80    8.77

192.168.13.57 configured, our_master, sane, valid, stratum 3
ref ID 192.168.1.111, time AFE252DC.1F2B3000 (00:12:28.121 PDT Mon Jul 5 1993)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 125.50 msec, root disp 115.80, reach 377, sync dist 186.157
delay 7.86 msec, offset 11.176 msec, dispersion 3.62
precision 2**6, version 2
org time AFE252DE.77C29000 (00:12:30.467 PDT Mon Jul 5 1993)
rcv time AFE252DE.7B2AE40B (00:12:30.481 PDT Mon Jul 5 1993)
xmt time AFE252DE.6E6D12E4 (00:12:30.431 PDT Mon Jul 5 1993)
filtdelay =    49.21    7.86    8.18    8.80    4.30    4.24    7.58    6.42
filtoffset =   11.30   11.18   11.13   11.28    8.91    9.09    9.27    9.57
filterror =     0.00    1.95    3.91    4.88    5.78    6.76    7.74    8.71
```

Table 85 describes the significant fields shown in the display.

Table 85 show ntp associations detail Field Descriptions

Field	Descriptions
configured	Peer was statically configured.
dynamic	Peer was dynamically discovered.

Table 85 show ntp associations detail Field Descriptions (continued)

Field	Descriptions
our_master	Local machine is synchronized to this peer.
selected	Peer is selected for possible synchronization.
candidate	Peer is a candidate for selection.
sane	Peer passes basic sanity checks.
insane	Peer fails basic sanity checks.
valid	Peer time is believed to be valid.
invalid	Peer time is believed to be invalid.
leap_add	Peer is signalling that a leap second will be added.
leap-sub	Peer is signalling that a leap second will be subtracted.
unsynced	Peer is not synchronized to any other machine.
ref ID	Address of machine peer is synchronized to.
time	Last time stamp peer received from its master.
our mode	Our mode relative to peer (active/passive/client/server/bdcast/bdcast client).
peer mode	Peer's mode relative to us.
our poll intvl	Our poll interval to peer.
peer poll intvl	Peer's poll interval to us.
root delay	Delay along path to root (ultimate stratum 1 time source).
root disp	Dispersion of path to root.
reach	Peer reachability (bit string in octal).
sync dist	Peer synchronization distance.
delay	Round-trip delay to peer.
offset	Offset of peer clock relative to our clock.
dispersion	Dispersion of peer clock.
precision	Precision of peer clock in Hertz.
version	NTP version number that peer is using.
org time	Originate time stamp.
rcv time	Receive time stamp.
xmt time	Transmit time stamp.
filtdelay	Round-trip delay (in milliseconds) of each sample.
filtoffset	Clock offset (in milliseconds) of each sample.
filterror	Approximate error of each sample.

Related Commands

Command	Description
show ntp status	Displays the status of the NTP.

show ntp status

To show the status of the Network Time Protocol (NTP), use the **show ntp status** command in Exec mode.

show ntp status

Syntax Description

This command has no arguments or keywords.

Command Mode

Exec

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample output from the **show ntp status** command:

```
Router> show ntp status

Clock is synchronized, stratum 4, reference is 192.168.13.57
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**19
reference time is AFE2525E.70597B34 (00:10:22.438 PDT Mon Jul 5 1993)
clock offset is 7.33 msec, root delay is 133.36 msec
root dispersion is 126.28 msec, peer dispersion is 5.98 msec
```

Table 86 describes the significant fields shown in the display.

Table 86 show ntp status Field Descriptions

Field	Description
synchronized	System is synchronized to an NTP peer.
unsynchronized	System is not synchronized to any NTP peer.
stratum	NTP stratum of this system.
reference	Address of peer the system is synchronized to.
nominal freq	Nominal frequency of system hardware clock.
actual freq	Measured frequency of system hardware clock.
precision	Precision of the clock of this system (in Hertz).
reference time	Reference time stamp.
clock offset	Offset of the system clock to synchronized peer.
root delay	Total delay along path to root clock.
root dispersion	Dispersion of root path.
peer dispersion	Dispersion of synchronized peer.

Related Commands

Command	Description
show ntp associations	Displays the status of the NTP associations.

show parser dump

To display the CLI syntax options for all command modes or for a specified command mode, use the **show parser dump** command in privileged Exec mode.

show parser dump {*command-mode* | **all**} [**privilege-level** *level*] [**extended**] [**breakage**]

Syntax Description

command-mode	A keyword indicating the command mode. The output will include the syntax for commands only in the specified command mode. The list of command mode keywords will vary depending on your software image. Use the **show parser dump ?** command to display the list of command mode keyword options. For further assistance determining the proper command mode, see the "Cisco IOS Command Modes" Release 12.2 document, available on Cisco.com.
all	Indicates that all commands in all modes should be displayed in the output. **Caution** This keyword generates a very large amount of output, which may exceed your system or buffer memory.
privilege-level *level*	(Optional) Lists CLI commands only with the privilege level specified in the level argument.
breakage	(Optional) Enables detection of potential parser chain syntax breakage. This keyword is intended for internal use.
extend	(Optional) Enables the extended display mode. The extended parser display shows the keyword and argument descriptions typically shown with the command-line help (**?** command). **Note** This keyword can produce a large amount of output.

Command Mode

Privileged Exec

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(13)T, 12.0(23)S	This command was enhanced to resolve certain execution errors.

Usage Guidelines

This command was developed to allow the exploration of the CLI command syntax without requiring the user to actually enter a specific mode and use the **?** command line help.

Caution Use caution when entering this command with the **all** keyword. A large amount of output can be generated by this command, which may easily exceed buffer or system memory on smaller platforms. Also, some configuration modes have hundreds of valid commands. For large dumps, use of the

redirection to a file using the **| redirect** *URL* syntax at the end of the command is highly recommended. (See the documentation for the **show <command> redirect** command for more information on using this command extension.)

Output for this command will show the syntax options for all commands available in the specified mode. The preceding number shows the privilege level associated with that command. For example, the line

```
15 type dhcp
```

indicates that the **type dhcp** command has a privilege level of 15 assigned to it. For information about privilege levels, see the "Configuring Passwords and Privileges" chapter in the *Cisco IOS Security Configuration Guide*.

Any given command-line string should indicate the full syntax needed to make the command complete and valid. In other words, the command line string ends where the carriage return (Enter) could be entered, as indicated in command-line help by the <cr> syntax. You will typically see multiple forms of a command, each showing a valid syntax combination. For example, each of the following syntax combinations, as seen in the output of the **show parser dump rtr | include dhcp** command, are valid commands:

```
type dhcp dest-ipaddr <address> source-ipaddr <address> option <82-82> circuit-id <string>
type dhcp dest-ipaddr <address> source-ipaddr <address> option <82-82> remote-id <string>
type dhcp dest-ipaddr <address> source-ipaddr <address> option <82-82> subnet-mask
<ipmask>
type dhcp dest-ipaddr <address> source-ipaddr <address> option <82-82>
type dhcp dest-ipaddr <address> source-ipaddr <address>
type dhcp dest-ipaddr <address>
type dhcp
```

Use of the show command extensions **| begin**, **| include**, and **| exclude** are recommended for this command, as these extensions allow you to filter the output to show only the commands you are interested in. The redirection extensions | **redirect**, | **append**, and | **tee** allow you to redirect the output of this command to local or remote storage as a file.

As with most **show** commands, you can typically exit from the --More-- prompt back to Exec mode using Ctrl-Z. For some connections, Ctrl-Shift-6 (Ctrl^) or Ctrl-Shift-6-X should be used instead.

Examples

The following example shows a typical list of command mode keywords:

```
Router# show parser dump ?
  aaa-user                  AAA user definition
  accept-dialin             VPDN group accept dialin configuration mode
  accept-dialout            VPDN group accept dialout configuration mode
  address-family            Address Family configuration mode
  aic                       Alarm Interface Card configuration mode
  all                       For all modes
  bba-group                 BBA Group configuration mode
  bsm-cfg                   BSM config definition
  cascustom                 Cas custom configuration mode
  clid-group                CLID group configuration mode
  cns-connect-intf-config   CNS Connect Intf Info Mode
  config-l2tp-class         l2tp-class configuration mode
  config-rtr-http-rr        RTR HTTP raw request Configuration
  config-x25-huntgroup      X.25 hunt group configuration mode
  configure                 Global configuration mode
  congestion                Frame Relay congestion configuration mode
  controller                Controller configuration mode
  dhcp                      DHCP pool configuration mode
```

```
dnis-group              DNIS group configuration mode
exec                    Exec mode
filter                  Output filter mode
filterserver            AAA filter server definitions
flow-cache              Flow aggregation cache config mode
flow-sampler-map        Flow sampler map config mode
fr-fr                   FR/FR connection configuration mode
frf5                    FR/ATM Network IWF configuration mode
frf8                    FR/ATM Service IWF configuration mode
interface               Interface configuration mode
interface               Interface range configuration mode
interface-dlci          Frame Relay dlci configuration mode
ip-vrf                  Configure IP VRF parameters
ipenacl                 IP named extended access-list configuration mode
ipnat-pool              IP NAT pool configuration mode
ipnat-snat              IP SNAT configuration mode
ipnat-snat-backup       IP SNAT Backup configuration mode
ipnat-snat-primary      IP SNAT Primary configuration mode
ipnat-snat-redundancy   IP SNAT Redundancy configuration mode
ipsnacl                 IP named simple access-list configuration mode
iua-cfg                 ISDN user adaptation layer configuration
key-chain               Key-chain configuration mode
key-chain-key           Key-chain key configuration mode
kron-occurrence         Kron Occurrence SubMode
kron-policy             Kron Policy SubMode
line                    Line configuration mode
lw-vlan-id              VLAN-id configuration mode
lw-vlan-range           VLAN-range configuration mode
map-class               Map class configuration mode
map-list                Map list configuration mode
mrm-manager             IP Multicast Routing Monitor config mode
null-interface          Null interface configuration mode
policy-list             IP Policy List configuration mode
preauth                 AAA Preauth definitions
qosclassmap             QoS Class Map configuration mode
qosclasspolice          QoS Class Police configuration mode
qospolicymap            QoS Policy Map configuration mode
qospolicymapclass       QoS Policy Map class configuration mode
radius-attrl            Radius Attribute-List Definition
red-group               random-detect group configuration mode
request-dialin          VPDN group request dialin configuration mode
request-dialout         VPDN group request dialout configuration mode
roles                   Role configuration mode
route-map               Route map config mode
router                  Router configuration mode
rsvp-local-policy       RSVP local policy configuration mode
rtr                     SAA entry configuration
saa-dhcp                SAA dhcp configuration
saa-dns                 SAA dns configuration
saa-echo                SAA echo configuration
saa-frameRelay          SAA FrameRelay configuration
saa-ftp                 SAA ftp configuration
saa-http                SAA http configuration
saa-jitter              SAA jitter configuration
saa-pathEcho            SAA pathEcho configuration
saa-pathJitter          SAA pathJitter configuration
saa-slm-ctrlr-if        SAA SLM controller/interface configuration
saa-slmFrIf             SAA SLM FrameRelay Interface configuration
saa-slmfr               SAA SLM Frame Relay configuration
saa-tcpConnect          SAA tcpConnect configuration
saa-udpEcho             SAA udpEcho configuration
sg-radius               Radius Server-group Definition
sg-tacacs+              Tacacs+ Server-group Definition
signaling-class         Signaling class configuration mode
```

```
  sss-subscriber          SSS subscriber configuration mode
  subinterface            Subinterface configuration mode
  subscriber-policy       Subscriber policy configuration mode
  tablemap                Table Map configuration mode
  tdm-conn                TDM connection configuration mode
  template                Template configuration mode
  tracking-config         Tracking configuration mode
  trange                  time-range configuration mode
  trunk-group             Trunk group configuration mode
  vc-class                VC class configuration mode
  vc-group                VC group configuration mode
  vlan                    VLAN database editing buffer
  vpdn-group              VPDN group configuration mode
  vpdn-template           VPDN template configuration mode
  x25-profile             X.25 profile configuration mode
```

In the following example, only commands in RTR Configuration mode are shown:

```
Router# show parser dump rtr
 Mode Name :rtr
15 type udpEcho dest-ipaddr <address> dest-port <1-65535> source-ipaddr <address>
source-port <1-65535> control enable
15 type udpEcho dest-ipaddr <address> dest-port <1-65535> source-ipaddr <address>
source-port <1-65535> control disable
15 type udpEcho dest-ipaddr <address> dest-port <1-65535> source-ipaddr <address>
source-port <1-65535>
15 type udpEcho dest-ipaddr <address> dest-port <1-65535> source-ipaddr <address>
15 type udpEcho dest-ipaddr <address> dest-port <1-65535>
15 type tcpConnect dest-ipaddr <address> dest-port <1-65535> source-ipaddr <address>
source-port <1-65535> control enable
15 type tcpConnect dest-ipaddr <address> dest-port <1-65535> source-ipaddr <address>
source-port <1-65535> control disable
15 type tcpConnect dest-ipaddr <address> dest-port <1-65535> source-ipaddr <address>
source-port <1-65535>
15 type tcpConnect dest-ipaddr <address> dest-port <1-65535> source-ipaddr <address>
15 type tcpConnect dest-ipaddr <address> dest-port <1-65535>
15 type jitter dest-ipaddr <address> dest-port <1-65535> source-ipaddr <address>
15 type jitter dest-ipaddr <address> dest-port <1-65535> source-port <1-65535>
15 type jitter dest-ipaddr <address> dest-port <1-65535> control enable
15 type jitter dest-ipaddr <address> dest-port <1-65535> control disable
15 type jitter dest-ipaddr <address> dest-port <1-65535> num-packets <1-60000>
15 type jitter dest-ipaddr <address> dest-port <1-65535> interval <1-60000>
15 type jitter dest-ipaddr <address> dest-port <1-65535>
15 type echo protocol ipIcmpEcho <address> source-ipaddr <address>
15 type echo protocol ipIcmpEcho <address>
15 type ftp operation get url <string> source-ipaddr <address> mode active
15 type ftp operation get url <string> source-ipaddr <address> mode passive
15 type ftp operation get url <string> source-ipaddr <address>
15 type ftp operation get url <string>
15 type http operation get url <string> name-server <address> version <string>
source-ipaddr <address> source-port <1-65535> cache
15 type http operation get url <string> name-server <address> version <string>
source-ipaddr <address> source-port <1-65535> cache
15 type http operation get url <string> name-server <address> version <string>
source-ipaddr <address> source-port <1-65535> cache
15 type http operation get url <string> name-server <address> version <string>
source-ipaddr <address> source-port <1-65535>
15 type http operation get url <string> name-server <address> version <string>
source-ipaddr <address>
15 type http operation get url <string> name-server <address> version <string>
15 type http operation get url <string> name-server <address>
15 type http operation get url <string>
15 type http operation raw
```

```
15 type dhcp dest-ipaddr <address> source-ipaddr <address> option <82-82> circuit-id
<string>
15 type dhcp dest-ipaddr <address> source-ipaddr <address> option <82-82> remote-id
<string>
15 type dhcp dest-ipaddr <address> source-ipaddr <address> option <82-82> subnet-mask
<ipmask>
15 type dhcp dest-ipaddr <address> source-ipaddr <address> option <82-82>
15 type dhcp dest-ipaddr <address> source-ipaddr <address>
15 type dhcp dest-ipaddr <address>
15 type dhcp
15 type dns target-addr <string> name-server <address> source-ipaddr <address> source-port
<1-65535>
15 type dns target-addr <string> name-server <address> source-ipaddr <address>
15 type dns target-addr <string> name-server <address>
15 type pathEcho protocol ipIcmpEcho <address> source-ipaddr <address>
15 type pathEcho protocol ipIcmpEcho <address>
15 type pathJitter dest-ipaddr <address> source-ipaddr <address>
15 type pathJitter dest-ipaddr <address> num-packets <1-100>
15 type pathJitter dest-ipaddr <address> interval <1-1000>
15 type pathJitter dest-ipaddr <address> targetOnly
15 type pathJitter dest-ipaddr <address>
15 type slm frame-relay pvc
15 type slm controller T1 <controller>
15 type slm controller E1 <controller>
15 type slm controller T3 <controller>
15 type slm controller E3 <controller>
15 exit
```

In the following example, only those commands in RTR Configuration mode containing the keyword **dhcp** are shown:

```
Router# show parser dump rtr | include dhcp
15 type dhcp dest-ipaddr <address> source-ipaddr <address> option <82-82> circuit-id
<string>
15 type dhcp dest-ipaddr <address> source-ipaddr <address> option <82-82> remote-id
<string>
15 type dhcp dest-ipaddr <address> source-ipaddr <address> option <82-82> subnet-mask
<ipmask>
15 type dhcp dest-ipaddr <address> source-ipaddr <address> option <82-82>
15 type dhcp dest-ipaddr <address> source-ipaddr <address>
15 type dhcp dest-ipaddr <address>
15 type dhcp
Router#
```

The following example shows how the **extend** keyword displays the syntax descriptions that match those shown using the ? command-line help:

```
Router# show parser dump rtr extend

 Mode Name :rtr
15 type udpEcho dest-ipaddr <address> dest-port <1-65535> source-ipaddr <address>
source-port <1-65535> control enable
type : Type of entry
udpEcho : UDP Echo Operation
dest-ipaddr : Destination address
<address> : IP address or hostname
dest-port : Destination Port
<1-65535> : Port Number
source-ipaddr : Source address
<address> : IP address or hostname
source-port : Source Port
<1-65535> : Port Number
control : Enable or disable control packets
```

```
enable : Enable control packets exchange (default)
 .
 .
 .
! Ctrl-Z used here to interrupt output and return to CLI prompt.

Router# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# rtr 1
Router(config-rtr)# type udpEcho ?
  dest-ipaddr  Destination address

Router(config-rtr)# type udpEcho dest-ipaddr ?
  Hostname or A.B.C.D  IP address or hostname

Router(config-rtr)# type udpEcho dest-ipaddr HOSTNAME ?
  dest-port  Destination Port

Router(config-rtr)# type udpEcho dest-ipaddr HOSTNAME dest-port ?
  <1-65535>  Port Number

Router(config-rtr)# type udpEcho dest-ipaddr HOSTNAME dest-port 1 ?
  control        Enable or disable control packets
  source-ipaddr  Source address
  source-port    Source Port
  <cr>

Router(config-rtr)# type udpEcho dest-ipaddr HOSTNAME dest-port 1 control ?
  disable  Disable control packets exchange
  enable  Enable control packets exchange (default)
```

In the following example, show parser dump output is redirected to a file on a remote TFTP server:

```
show parser dump exec extend | redirect
tftp://209.165.200.225/userdirectory/123-exec-commands.txt
```

Related Commands

Command	Description
show <command> append	Redirects and adds the output of any **show** command to an existing file.
show <command> redirect	Redirects the output of any **show** command to a file.
show <command> tee	Copies the output of any **show** command to a file while displaying it on the terminal.
show <command> include	Filters **show** command output so that only lines that containing the specified string are displayed.
show <command> begin	Filters the output of any **show** command to display the output from the first instance of a specified string.
show <command> exclude	Filters **show** command output so that it excludes lines that contain a particular regular expression.

show parser statistics

To displays statistics about the last configuration file parsed and the status of the Parser Cache feature, use the **show parser statistics** command in privileged Exec mode.

show parser statistics

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged Exec

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

The **show parser statistics** command displays two sets of data:

- The number of commands in the configuration file that was last copied into the running configuration, and the time it took for the system to parse them (a configuration file can be loaded into the running configuration at system startup, or by issuing commands such as the **copy** *source* **running-config** command).
- The status of the Parser Cache feature (enabled or disabled) and the number of command matches (indicated by hits/misses) since the system was started or since the parser cache was cleared.

The Parser Cache feature optimizes the parsing (translation and execution) of Cisco IOS software configuration command lines by remembering how to parse recently encountered command lines, decreasing the time required to process large configuration files.

Examples

The following example shows sample output from the **show parser statistics** command:

```
Router# show parser statistics

Last configuration file parsed:Number of Commands:1484, Time:1272 ms

Parser cache:disabled, 0 hits, 2 misses
```

In this example, the Parser Cache feature is disabled, but shows the hit/miss statistics for the two commands issued while the parser cache was last enabled.

Table 87 describes the key output fields.

Table 87 show parser statistics Output Fields

Last configuration file parsed:	Displays statistics on the last configuration file copied into the running configuration (at startup or using the **copy** command).
Number of commands:	The number of command lines in the last configuration file parsed.
Time:	Time (in milliseconds) taken for the system to load the last configuration file.
Parser cache:	Displays whether the Parser Cache feature is enabled or disabled, and the hit/miss statistics related to the feature. Statistics are stored since the initialization of the system, or since the last time the parser cache was cleared.
hits	Number of commands the parser cache was able to parse more efficiently by matching them to similar commands executed previously.
misses	Number of commands the parser cache was unable to match to previously executed commands. The performance enhancement provided by the Parser Cache feature cannot be applied to unmatched commands.

In the following example the **show parser statistics** command is used to compare the parse-time of a large configuration file with the Parser Cache feature disabled and enabled. In this example, a configuration file with 1484 access list commands is loaded into the running configuration.

```
Router# configure terminal
!parser cache is disabled
Router(config)# no parser cache
!configuration file is loaded into the running configuration
Router# copy slot0:acl_list running-config
.
.
.
Router# show parser statistics
Last configuration file parsed:Number of Commands:1484, Time:1272 ms

Parser cache:disabled, 0 hits, 2 misses

!the parser cache is reenabled
Router(config)# parser cache
!configuration file is loaded into the running configuration
Router# copy slot0:acl_list running-config
.
.
.
Router# show parser statistics
Last configuration file parsed:Number of Commands:1484, Time:820 ms

Parser cache:enabled, 1460 hits, 26 misses
```

These results show an improvement to the load time for the same configuration file from 1272 milliseconds (ms) to 820 ms when the Parser Cache feature was enabled. As indicated in the "hits" field of the **show** command output, 1460 commands were able to be parsed more efficiently by the parser cache.

Related Commands

Command	Description
clear parser cache	Clears the parse cache entries and hit/miss statistics stored for the Parser Cache feature.
parser cache	Enables or disables the Parser Cache feature.

show pci

To display information about the peripheral component interconnect (PCI) hardware registers or bridge registers for the Cisco 7200 series routers, use the **show pci** command in Exec mode.

show pci {**hardware** | **bridge** [*register*]}

Syntax Description

hardware	Displays PCI hardware registers.
bridge	Displays PCI bridge registers.
register	(Optional) Number of a specific bridge register in the range from 0 to 7. If not specified, this command displays information about all registers.

Command Mode

Exec

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The output of this command is generally useful for diagnostic tasks performed by technical support only.

Note The **show pci hardware** Exec command displays a substantial amount of information.

Examples

The following is sample output for the PCI bridge register 1 on a Cisco 7200 series router:

```
Router# show pci bridge 1

Bridge 4, Port Adaptor 1, Handle=1
DEC21050 bridge chip, config=0x0
(0x00): cfid   = 0x00011011
(0x04): cfcs   = 0x02800147
(0x08): cfccid = 0x06040002
(0x0C): cfpmlt = 0x00010010

(0x18): cfsmlt = 0x18050504
(0x1C): cfsis  = 0x22805050
(0x20): cfmla  = 0x48F04880
(0x24): cfpmla = 0x00004880

(0x3C): cfbc   = 0x00000000
(0x40): cfseed = 0x00100000
(0x44): cfstwt = 0x00008020
```

The following is partial sample output for the PCI hardware register, which also includes information on all the PCI bridge registers on a Cisco 7200 series router:

```
Router# show pci hardware

GT64010 External PCI Configuration registers:
```

```
 Vendor / Device ID   : 0xAB114601 (b/s 0x014611AB)
 Status / Command     : 0x17018002 (b/s 0x02800117)
 Class / Revision     : 0x00000006 (b/s 0x06000000)
 Latency              : 0x0F000000 (b/s 0x0000000F)
 RAS[1:0] Base        : 0x00000000 (b/s 0x00000000)
 RAS[3:2] Base        : 0x00000001 (b/s 0x01000000)
 CS[2:0] Base         : 0x00000000 (b/s 0x00000000)
 CS[3] Base           : 0x00000000 (b/s 0x00000000)
 Mem Map Base         : 0x00000014 (b/s 0x14000000)
 IO Map Base          : 0x01000014 (b/s 0x14000001)
 Int Pin / Line       : 0x00010000 (b/s 0x00000100)

Bridge 0, Downstream MB0 to MB1, Handle=0
DEC21050 bridge chip, config=0x0
(0x00): cfid   = 0x00011011
(0x04): cfcs   = 0x02800143
(0x08): cfccid = 0x06040002
(0x0C): cfpmlt = 0x00011810

(0x18): cfsmlt = 0x18000100
(0x1C): cfsis  = 0x02809050
(0x20): cfmla  = 0x4AF04880
(0x24): cfpmla = 0x4BF04B00

(0x3C): cfbc   = 0x00000000
(0x40): cfseed = 0x00100000
(0x44): cfstwt = 0x00008020
.
.
.
```

show pci hardware

To display information about the Host-PCI bridge, use the **show pci hardware** command in Exec mode.

show pci hardware

Syntax Description

This command has no arguments or keywords.

Command Mode

Exec

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The output of this command is generally useful for diagnostic tasks performed by technical support only:

```
Router# show pci hardware

hardware PCI hardware registers

Each device on the PCI bus is assigned a PCI device number.  For the
C2600, device numbers are as follows:

Device    Device number
0         First LAN device
1         Second LAN device
2         AIM device (if present)
3         Not presently used
4         Port module - first PCI device
5         Port module - second PCI device
6         Port module - third PCI device
7         Port module - fourth PCI device
8-14      Not presently used
15        Xilinx PCI bridge
```

Examples

The following is partial sample output for the PCI hardware register, which also includes information on all the PCI bridge registers.

```
router# show pci hardware

XILINX Host-PCI Bridge Registers:
Vendor / Device ID: 0x401310EE
Status / Command: 0x040001C6
PCI Slave Base Reg 0: 0x00000000
PCI Slave Base Reg 1: 0x04000000
```

Table 88 describes the significant fields shown in the display.

Table 88 show pci hardware Field Descriptions

Field	Description
Device/Vendor ID	Identifies the PCI vendor and device. The value 0x401310EE identifies the device as the Xilinx-based Host-PCI bridge for the Cisco 2600 router.
Status/Command	Provides status of the Host-PCI bridge. Refer to the PCI Specification for more information.
PCI Slave Base Reg 0	The base address of PCI Target Region 0 for the Host-PCI bridge. This region is used for Big-Endian transfers between PCI devices and memory.
PCI Slave Base Reg 1	The base address of PCI Target Region 1 for the Host-PCI bridge. This region is used for Little-Endian transfers between PCI devices and memory.

show processes

To display information about the active processes, use the **show processes** command in Exec mode.

show processes [**cpu**]

Syntax Description

cpu	(Optional) Displays detailed central processing unit (CPU) utilization statistics (CPU use per process).

Command Mode

Exec

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample output from the **show processes** command:

```
Router# show processes

CPU utilization for five seconds: 21%/0%; one minute: 2%; five minutes: 2%
PID QTy       PC Runtime (ms)   Invoked   uSecs     Stacks    TTY  Process
  1 Mwe  2FEA4E         1808       464    3896     1796/3000   0  IP-EIGRP Router
  2 Lst  11682          10236      109   93908     1828/2000   0  Check heaps
  3 Mst  3AE9C              0      280       0     1768/2000   0  Timers
  4 Lwe  74AD2              0       12       0     1492/2000   0  ARP Input
  5.ME   912E4              0        2       0     1892/2000   0  IPC Zone Manager
  6.ME   91264              0        1       0     1936/2000   0  IPC Realm Manager
  7.ME   91066              0       30       0     1784/2000   0  IPC Seat Manager
  8.ME  133368              0        1       0     1928/2000   0  CXBus hot stall
  9.ME  1462EE              0        1       0     1940/2000   0 Microcode load
 10 Msi 127538              4       76      52     1608/2000   0 Env Mon
 11.ME  160CF4              0        1       0     1932/2000   0 MIP Mailbox
 12 Mwe 125D7C              4      280      14     1588/2000   0 SMT input
 13 Lwe AFD0E               0        1       0     1772/2000   0 Probe Input
 14 Mwe AF662               0        1       0     1784/2000   0 RARP Input
 15 Hwe A1F9A             228      549     415     3240/4000   0 IP Input
 16 Msa C86A0               0      114       0     1864/2000   0 TCP Timer
 17 Lwe CA700               0        1       0     1756/2000   0 TCP Protocols
 18.ME  CCE7C               0        1       0     1940/2000   0 TCP Listener
 19 Mwe AC49E               0        1       0     1592/2000   0 BOOTP Server
 20 Mwe 10CD84             24       77     311     1652/2000   0 CDP Protocol
 21 Mwe 27BF82              0        2       0     1776/2000   0 ATMSIG Input
```

Table 89 describes the significant fields shown in the output.

The following is sample output from the **show processes cpu** command:

```
Router# show processes cpu
CPU utilization for five seconds: 5%/2%; one minute: 3%; five minutes: 2%
  PID  Runtime (ms)    Invoked   uSecs   5Sec  1Min  5Min  TTY Process
    1          1736         58   29931     0%    0%    0%  Check heaps
    2            68        585     116  1.00% 1.00%    0%  IP Input
    3             0        744       0     0%    0%    0%  TCP Timer
    4             0          2       0     0%    0%    0%  TCP Protocols
```

```
  5           0           1           0     0%    0%    0%  BOOTP Server
  6          16         130         123     0%    0%    0%   ARP Input
  7           0           1           0     0%    0%    0%  Probe Input
  8           0           7           0     0%    0%    0%  MOP Protocols
  9           0           2           0     0%    0%    0%  Timers
 10         692          64       10812     0%    0%    0%  Net Background
 11           0           5           0     0%    0%    0%  Logger
 12           0          38           0     0%    0%    0%  BGP Open
 13           0           1           0     0%    0%    0%  Net Input
 14         540        3466         155     0%    0%    0%  TTY Background
 15           0           1           0     0%    0%    0%  BGP I/O
 16        5100        1367        3730     0%    0%    0%  IGRP Router
 17          88        4232          20  0.20% 1.00%    0%  BGP Router
 18         152       14650          10     0%    0%    0%  BGP Scanner
 19         224          99        2262     0%    0% 1.00%  Exec
```

Table 89 describes the significant fields shown in the display.

Table 89 show processes Field Descriptions

Field	Description
CPU utilization for five seconds	CPU utilization for the last 5 seconds. The second number indicates the percent of CPU time spent at the interrupt level.
one minute	CPU utilization for the last minute.
five minutes	CPU utilization for the last 5 minutes.
PID	Process ID.
Q	Process queue priority. Possible values: C (critical), H (high), M (medium), L (low).
Ty	Scheduler test. Possible values: * (currently running), E (waiting for an event), S (ready to run, voluntarily relinquished processor), rd (ready to run, wakeup conditions have occurred), we (waiting for an event), sa (sleeping until an absolute time), si (sleeping for a time interval), sp (sleeping for a time interval (alternate call), st (sleeping until a timer expires), hg (hung; the process will never execute again), xx (dead: the process has terminated, but has not yet been deleted.).
PC	Current program counter.
Runtime (ms)	CPU time the process has used (in milliseconds).
Invoked	Number of times the process has been invoked.
uSecs	Microseconds of CPU time for each process invocation.
Stacks	Low water mark/Total stack space available (in bytes).
TTY	Terminal that controls the process.
Process	Name of the process.
5Sec	CPU utilization by task in the last 5 seconds.
1Min	CPU utilization by task in the last minute.
5Min	CPU utilization by task in the last 5 minutes.

Note Because the network server has a 4-millisecond clock resolution, run times are considered reliable only after a large number of invocations or a reasonable, measured run time.

Related Commands

Command	Description
show processes memory	Displays amount of system memory used per system process.

show processes memory

To show memory used, use the **show processes memory** command in Exec mode.

show processes memory

Syntax Description

This command has no arguments or keywords.

Command Mode

Exec

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample output from the **show processes memory** command:

```
Router# show processes memory

Total: 5611448, Used: 2307548, Free: 3303900
 PID  TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
   0    0     199592       1236    1907220          0          0 *Init*
   0    0        400      76928        400          0          0 *Sched*
   0    0    5431176    3340052     140760     349780          0 *Dead*
   1    0        256        256       1724          0          0 Load Meter
   2    0        264          0       5032          0          0 Exec
   3    0          0          0       2724          0          0 Check heaps
   4    0      97932          0       2852      32760          0 Pool Manager
   5    0        256        256       2724          0          0 Timers
   6    0         92          0       2816          0          0 CXBus hot stall
   7    0          0          0       2724          0          0 IPC Zone Manager
   8    0          0          0       2724          0          0 IPC Realm Manager
   9    0          0          0       2724          0          0 IPC Seat Manager
  10    0        892        476       3256          0          0 ARP Input
  11    0         92          0       2816          0          0 SERIAL A'detect
  12    0        216          0       2940          0          0 Microcode Loader
  13    0          0          0       2724          0          0 RFSS watchdog
  14    0   15659136   15658584       3276          0          0 Env Mon
.
.
.
  77    0        116          0       2844          0          0 IPX-EIGRP Hello
                                    2307224 Total
```

Table 90 describes the significant fields shown in the display.

Table 90 show processes memory Field Descriptions

Field	Description
Total	Total amount of memory held.
Used	Total amount of used memory.
Free	Total amount of free memory.

Table 90 show processes memory Field Descriptions (continued)

Field	Description
PID	Process ID.
TTY	Terminal that controls the process.
Allocated	Bytes of memory allocated by the process.
Freed	Bytes of memory freed by the process, regardless of who originally allocated it.
Holding	Amount of memory currently allocated to the process.
Getbufs	Number of times the process has requested a packet buffer.
Retbufs	Number of times the process has relinquished a packet buffer.
Process	Process name.
Init	System initialization.
Sched	The scheduler.
Dead	Processes as a group that are now dead.
Total	Total amount of memory held by all processes.

Related Commands

Command	Description
show memory	Displays statistics about memory, including memory-free pool statistics.
show processes	Displays information about the active processes.

show protocols

To display the configured protocols, use the **show protocols** command in Exec mode.

This command shows the global and interface-specific status of any configured Level 3 protocol; for example, IP, DECnet, IPX, AppleTalk, and so on.

show protocols

Syntax Description

This command has no arguments or keywords.

Command Mode

Exec

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample output from the **show protocols** command:

```
Router# show protocols

Global values:
  Internet Protocol routing is enabled
  DECNET routing is enabled
  XNS routing is enabled
  Appletalk routing is enabled
  X.25 routing is enabled
Ethernet 0 is up, line protocol is up
  Internet address is 192.168.1.1, subnet mask is 255.255.255.0
  Decnet cost is 5
  XNS address is 2001.AA00.0400.06CC
  AppleTalk address is 4.129, zone Twilight
Serial 0 is up, line protocol is up
  Internet address is 192.168.7.49, subnet mask is 255.255.255.240
Ethernet 1 is up, line protocol is up
  Internet address is 192.168.2.1, subnet mask is 255.255.255.0
  Decnet cost is 5
  XNS address is 2002.AA00.0400.06CC
  AppleTalk address is 254.132, zone Twilight
Serial 1 is down, line protocol is down
  Internet address is 192.168.7.177, subnet mask is 255.255.255.240
  AppleTalk address is 999.1, zone Magnolia Estates
```

For more information on the parameters or protocols shown in this sample output, see the *Cisco IOS Network Protocols Configuration Guide, Part 1*, *Network Protocols Configuration Guide, Part 2*, and *Network Protocols Configuration Guide, Part 3*.

show region

To display valid memory regions (memory mapping) in use on your system, use the **show region** command in Privileged Exec mode.

show region [**address** *hex-address*]

Syntax Description

address *hex-address*	(Optional) If a hex address is specified, this command will search the region list for the specified address.

Defaults

All memory regions are displayed.

Command Modes

Privileged Exec

Command History

Release	Modification
12.1, 12.0(9)S	**Show region** output was made available in the output of the **show technical-support** command.
12.2(15)ZN, 12.2(15)BZ, 12.1(14)E, 12.2(13)S, 12.2(13), 12.2(13)T, 12.0(23)S	The **show region** command was enabled as an independant command.

Usage Guidelines

This command can be useful for troubleshooting system bus errors. The system encounters a bus error when the processor tries to access a memory location that either does not exist (a software error) or does not respond properly (a hardware problem).

To use the show region command to troubleshoot a bus error, note the memory location address from the **show version** command, the **show context** command, or from the system error message that alerted you to the bus error. The show region command can then be used to determine if that address is a valid memory location.

For example, in the output of the **show version** command after a system restart casued by a bus error, you will see output similar to "System restarted by bus error at PC 0x30EE546, address 0xBB4C4." In this case, the memory location that the router tried to access is 0xBB4C4. If the address falls within one of the ranges in the **show region** output, it means that the router was accessing a valid memory address, but the hardware corresponding to that address is not responding properly. This indicates a hardware problem.

If the address reported by the bus error does not fall within the ranges displayed in the **show region** output, this means that the router was trying to access an address that is not valid. This indicates that it is a Cisco IOS Software problem.

More detailed information is available on Cisco.com in Tech Note #7949, *Troubleshooting Bus Error Crashes*.

Examples

The following is sample output from the **show region** command:

```
Router# show region

Region Manager:

      Start         End      Size(b)  Class  Media  Name
 0x40000000  0x40001FFF         8192  Iomem  REG    qa
 0x40002000  0x401FFFFF      2088960  Iomem  R/W    memd
 0x48000000  0x48001FFF         8192  Iomem  REG    qa:writethru
 0x50002000  0x501FFFFF      2088960  Iomem  R/W    memd:(memd_bitswap)
 0x58002000  0x581FFFFF      2088960  Iomem  R/W    memd:(memd_uncached)
 0x60000000  0x6FFFFFFF    268435456  Local  R/W    main
 0x600109C8  0x611BEBE1     18539034  IText  R/O    main:text
 0x611C0000  0x61642C7F      4729984  IData  R/W    main:data
 0x61642C80  0x6186607F      2241536  IBss   R/W    main:bss
 0x61866080  0x6188607F       131072  Local  R/W    main:fastheap
 0x61886080  0x6FFFFFFF    242720640  Local  R/W    main:heap
 0x80000000  0x87FFFFFF    134217728  Local  R/W    main:(main_k0)
 0x88000000  0x88001FFF         8192  Iomem  REG    qa_k0
 0x88002000  0x881FFFFF      2088960  Iomem  R/W    memd:(memd_k0)
 0xA0000000  0xA7FFFFFF    134217728  Local  R/W    main:(main_k1)
 0xA8000000  0xA8001FFF         8192  Iomem  REG    qa_k1
 0xA8002000  0xA81FFFFF      2088960  Iomem  R/W    memd:(memd_k1)
```

Related Commands

Command	Description
show context	Displays information stored in NVRAM when an unexpected system reload (system exception) occurs.
show memory	Displays detailed memory statistics for the system.
show version	Shows hardware and software information for the system.

show registry

To show the function registry information, use the **show registry** command in Exec mode.

show registry [*registry-name* [*registry-number*]] [**brief** | **statistics**]

Syntax Description

registry-name	(Optional) Name of the registry to examine.
registry-number	(Optional) Number of the registry to examine.
brief	(Optional) Displays limited functions and services information.
statistics	(Optional) Displays function registry statistics.

Command Mode

Exec

Command History

Release	Modification
11.1	This command was introduced.

Examples

The following is sample output from the **show registry** command using the **brief** keyword:

```
Router> show registry atm 3/0/0 brief

Registry objects: 1799  bytes: 213412

--
Registry 23: ATM Registry
  Service 23/0:
  Service 23/1:
  Service 23/2:
  Service 23/3:
  Service 23/4:
  Service 23/5:
  Service 23/6:
  Service 23/7:
  Service 23/8:
  Service 23/9:
  Service 23/10:
  Service 23/11:
  Service 23/12:
  Service 23/13:
  Service 23/14:

--
RegistrY 25: ATM routing Registry
  Service 25/0:
```

show reload

To display the reload status on the router, use the **show reload** command in Exec mode.

show reload

Syntax Description

This command has no arguments or keywords.

Command Mode

Exec

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

You can use the **show reload** command to display a pending software reload. To cancel the reload, use the **reload cancel** privileged Exec command.

Examples

The following sample output from the **show reload** command shows that a reload is schedule for 12:00 a.m. (midnight) on Saturday, April 20:

```
Router# show reload

Reload scheduled for 00:00:00 PDT Sat April 20 (in 12 hours and 12 minutes)
Router#
```

Related Commands

Command	Description
reload	Reloads the operating system.

show rmon

To display the current RMON agent status on the router, use the **show rmon** command in Exec mode.

show rmon [**alarms** | **capture** | **events** | **filter** | **history** | **hosts** | **matrix** | **statistics** | **task** | **topn**]

Syntax Description

alarms	(Optional) Displays the RMON alarm table.
capture	(Optional) Displays the RMON buffer capture table. Available on Cisco 2500 series and Cisco AS5200 series only.
events	(Optional) Displays the RMON event table.
filter	(Optional) Displays the RMON filter table. Available on Cisco 2500 series and Cisco AS5200 series only.
history	(Optional) Displays the RMON history table. Available on Cisco 2500 series and Cisco AS5200 series only.
hosts	(Optional) Displays the RMON hosts table. Available on Cisco 2500 series and Cisco AS5200 series only.
matrix	(Optional) Displays the RMON matrix table. Available on Cisco 2500 series and Cisco AS5200 series only.
statistics	(Optional) Displays the RMON statistics table. Available on Cisco 2500 series and Cisco AS5200 series only.
task	(Optional) Displays general RMON statistics. This is the default.
topn	(Optional) Displays the RMON top-n hosts table. Available on Cisco 2500 series and Cisco AS5200 series only.

Defaults

If no option is specified, the **task** option is displayed.

Command Mode

Exec

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Refer to the specific **show rmon** command for an example and description of the fields.

For additional information, refer to the RMON MIB described in RFC 1757.

Examples

The following is sample output from the **show rmon** command. All counters are from the time the router was initialized.

```
Router# show rmon

145678 packets input (34562 promiscuous), 0 drops
145678 packets processed, 0 on queue, queue utilization 15/64
```

Table 91 describes the significant fields shown in the ouput.

Table 91 show rmon Field Descriptions

Field	Description
x packets input	Number of packets received on RMON-enabled interfaces.
x promiscuous	Number of input packets that were seen by the router only because RMON placed the interface in promiscuous mode.
x drops	Number of input packets that could not be processed because the RMON queue overflowed.
x packets processed	Number of input packets actually processed by the RMON task.
x on queue	Number of input packets that are sitting on the RMON queue, waiting to be processed.
queue utilization *x*/*y*	*y* is the maximum size of the RMON queue; *x* is the largest number of packets that were ever on the queue at a particular time.

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
rmon alarm	Sets an alarm on any MIB object.
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.
rmon queuesize	Changes the size of the queue that holds packets for analysis by the RMON process.
show rmon alarms	Displays the contents of the router's RMON alarm table.
show rmon capture	Displays the contents of the router's RMON capture table.
show rmon events	Displays the contents of the router's RMON event table.
show rmon filter	Displays the contents of the router's RMON filter table.
show rmon history	Displays the contents of the router's RMON history table.
show rmon hosts	Displays the contents of the router's RMON hosts table.
show rmon matrix	Displays the contents of the router's RMON matrix table.
show rmon statistics	Displays the contents of the router's RMON statistics table.
show rmon topn	Displays the contents of the router's RMON p-N host table.

show rmon alarms

To display the contents of the RMON alarm table of the router, use the **show rmon alarms** command in Exec mode.

show rmon alarms

Syntax Description

This command has no arguments or keywords.

Command Mode

Exec

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

For additional information, refer to the RMON MIB described in RFC 1757.

You must have first enabled RMON on the interface, and configured RMON alarms to display alarm information with the **show rmon alarms** command.

Examples

The following is sample output from the **show rmon alarms** command:

```
Router# show rmon alarms

Alarm 2 is active, owned by manager1
 Monitors ifEntry.1.1 every 30 seconds
 Taking delta samples, last value was 0
 Rising threshold is 15, assigned to event 12
 Falling threshold is 0, assigned to event 0
 On startup enable rising or falling alarm
```

Table 92 describes the significant fields shown in the display.

Table 92 show rmon alarms Field Descriptions

Field	Description
Alarm 2 is active, owned by manager1	Unique index into the alarmTable, showing the alarm status is active, and the owner of this row, as defined in the alarmTable of RMON.
Monitors ifEntry.1.1	Object identifier of the particular variable to be sampled. Equivalent to alarmVariable in RMON.
every 30 seconds	Interval in seconds over which the data is sampled and compared with the rising and falling thresholds. Equivalent to alarmInterval in RMON.
Taking delta samples	Method of sampling the selected variable and calculating the value to be compared against the thresholds. Equivalent to alarmSampleType in RMON.

Table 92 show rmon alarms Field Descriptions (continued)

Field	Description
last value was	Value of the statistic during the last sampling period. Equivalent to alarmValue in RMON.
Rising threshold is	Threshold for the sampled statistic. Equivalent to alarmRisingThreshold in RMON.
assigned to event	Index of the eventEntry that is used when a rising threshold is crossed. Equivalent to alarmRisingEventIndex in RMON.
Falling threshold is	Threshold for the sampled statistic. Equivalent to alarmFallingThreshold in RMON.
assigned to event	Index of the eventEntry that is used when a falling threshold is crossed. Equivalent to alarmFallingEventIndex in RMON.
On startup enable rising or falling alarm	Alarm that may be sent when this entry is first set to valid. Equivalent to alarmStartupAlarm in RMON.

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
rmon alarm	Sets an alarm on any MIB object.
show rmon	Displays the current RMON agent status on the router.

show rmon capture

To display the contents of the router's RMON capture table, use the **show rmon capture** command in Exec mode.

show rmon capture

Syntax Description

This command has no arguments or keywords.

Command Mode

Exec

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

For additional information, refer to the RMON MIB described in RFC 1757.

You must have first enabled RMON on the interface, and configured RMON alarms and events to display alarm information with the **show rmon capture** command.

This command is available on the Cisco 2500 series and Cisco AS5200 series only.

Examples

The following is sample output from the **show rmon capture** command:

```
Router# show rmon capture

Buffer 4096 is active, owned by manager1
 Captured data is from channel 4096
 Slice size is 128, download size is 128
 Download offset is 0
 Full Status is spaceAvailable, full action is lockWhenFull
 Granted 65536 octets out of 65536 requested
 Buffer has been on since 00:01:16, and has captured 1 packets
  Current capture buffer entries:
   Packet 1 was captured 416 ms since buffer was turned on
   Its length is 326 octets and has a status type of 0
   Packet ID is 634, and contains the following data:
00 00 0c 03 12 ce 00 00 0c 08 9d 4e 08 00 45 00
01 34 01 42 00 00 1d 11 e3 01 ab 45 30 15 ac 15
31 06 05 98 00 a1 01 20 9f a8 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00
```

Table 93 describes the significant fields shown in the ouput.

Table 93 show rmon capture Field Descriptions

Field	Description
Buffer 4096 is active	Equates to bufferControlIndex in the bufferControlTable of RMON. Uniquely identifies a valid (active) row in this table.
owned by manager1	Denotes the owner of this row. Equates to bufferControlOwner in the bufferControlTable of RMON.
Captured data is from channel	Equates to the bufferControlChannelIndex and identifies which RMON channel is the source of these packets.
Slice size is	Identifies the maximum number of octets of each packet that will be saved in this capture buffer. Equates to bufferControlCaptureSliceSize of RMON.
download size is	Identifies the maximum number of octets of each packet in this capture buffer that will be returned in an SNMP retrieval of that packet. Equates to bufferControlDownloadSliceSize in RMON.
Download offset is	Offset of the first octet of each packet in this capture buffer that will be returned in an SNMP retrieval of that packet. Equates to bufferControlDownloadOffset in RMON.
Full Status is spaceAvailable	Shows whether the buffer is full or has room to accept new packets. Equates to bufferControlFullStatus in RMON.
full action is lockWhenFull	Controls the action of the buffer when it reaches full status. Equates to bufferControlFullAction in RMON.
Granted 65536 octets	Actual maximum number of octets that can be saved in this capture buffer. Equates to bufferControlMaxOctetsGranted in RMON.
out of 65536 requested	Requested maximum number of octets to be saved in this capture buffer. Equates to bufferControlMaxOctetsRequested in RMON.
Buffer has been on since	Indicates how long the buffer has been available.
and has captured 1 packets	Number of packets captured since buffer was turned on. Equates to bufferControlCapturedPackets in RMON.
Current capture buffer entries:	Lists each packet captured.
Packet 1 was captured 416 ms since buffer was turned on Its length is 326 octets and has a status type of 0	Zero indicates the error status of this packet. Equates to captureBufferPacketStatus in RMON, where its value options are documented.
Packet ID is	Index that describes the order of packets received on a particular interface. Equates to captureBufferPacketID in RMON.
and contains the following data:	Data inside the packet, starting at the beginning of the packet.

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
rmon alarm	Sets an alarm on any MIB object.
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.
show rmon	Displays the current RMON agent status on the router.

show rmon events

To display the contents of the router's RMON event table, use the **show rmon events** command in Exec mode.

show rmon events

Syntax Description

This command has no arguments or keywords.

Command Mode

Exec

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

For additional information, refer to the RMON MIB described in RFC 1757.

You must have first enabled RMON on the interface, and configured RMON events to display alarm information with the **show rmon events** command.

Examples

The following is sample output from the **show rmon events** command:

```
Router# show rmon events

Event 12 is active, owned by manager1
 Description is interface-errors
 Event firing causes log and trap to community rmonTrap, last fired 00:00:00
```

Table 94 describes the significant fields shown in the display.

Table 94 show rmon events Field Descriptions

Field	Description
Event 12 is active, owned by manager1	Unique index into the eventTable, showing the event status is active, and the owner of this row, as defined in the eventTable of RMON.
Description is interface-errors	Type of event, in this case an interface error.
Event firing causes log and trap	Type of notification that the router will make about this event. Equivalent to eventType in RMON.
community rmonTrap	If an SNMP trap is to be sent, it will be sent to the SNMP community specified by this octet string. Equivalent to eventCommunity in RMON.
last fired	Last time the event was generated.

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.
show rmon	Displays the current RMON agent status on the router.

show rmon filter

To display the contents of the router's RMON filter table, use the **show rmon filter** command in Exec mode.

Syntax Description

This command has no arguments or keywords.

Command Mode

Exec

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

For additional information, refer to the RMON MIB described in RFC 1757.

You must have first enabled RMON on the interface, and configured RMON alarms and events to display alarm information with the **show rmon filter** command.

This command is available on the Cisco 2500 series and Cisco AS5200 series only.

Examples

The following is sample output from the **show rmon filter** command:

```
Router# show rmon filter

Filter 4096 is active, and owned by manager1
 Data offset is 12, with
 Data of  08 00 00 00 00 00 00 00 00 00 00 00 00 ab 45 30 15 ac 15 31 06
 Data Mask is ff ff 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff
 Data Not Mask is 0
 Pkt status is 0, status mask is 0, not mask is 0
 Associated channel 4096 is active, and owned by manager1
 Type of channel is acceptFailed, data control is off
 Generate event index 0
 Event status is eventFired, # of matches is 1482
 Turn on event index is 0, turn off event index is 0
 Description:
```

Table 95 describes the significant fields shown in the display.

Table 95 show rmon filter Field Descriptions

Field	Description
Filter *x* is active, and owned by *y*	Unique index of the filter, its current state, and the owner, as defined in the filterTable of RMON.
Data offset is	Offset from the beginning of each packet where a match of packet data will be attempted. Equivalent to filterPktDataOffset in RMON.

Table 95 show rmon filter Field Descriptions (continued)

Field	Description
Data of	Data that is to be matched with the input packet. Equivalent to filterPktData in RMON.
Data Mask is	Mask that is applied to the match process. Equivalent to filterPktDataMask in RMON.
Data Not Mask is	Inversion mask that is applied to the match process. Equivalent to filterPktDataNotMask in RMON.
Pkt status is	Status that is to be matched with the input packet. Equivalent to filterPktStatus in RMON.
status mask is	Mask that is applied to the status match process. Equivalent to filterPktStatusMask in RMON.
not mask is	Inversion mask that is applied to the status match process. Equivalent to filterPktStatusNotMask in RMON.
Associated channel *x* is active, and owned by *y*	Unique index of the channel, its current state, and the owner, as defined in the channelTable of RMON.
Type of channel is {acceptMatched | acceptFailed}	This object controls the action of the filters associated with this channel. Equivalent to channelAcceptType of RMON.
data control is {off | on }	This object controls the flow of data through this channel. Equivalent to channelDataControl in RMON.
Generate event index 0	Value of this object identifies the event that is configured to be generated when the associated channelDataControl is on and a packet is matched. Equivalent to channelEventIndex in RMON.
Event status is eventFired	When the channel is configured to generate events when packets are matched, this message indicates the means of controlling the flow of those events. Equivalent to channelEventStatus in RMON.
# of matches is	Number of times this channel has matched a packet. Equivalent to channelMatches in RMON.
Turn on event index is	Value of this object identifies the event that is configured to turn the associated channelDataControl from off to on when the event is generated. Equivalent to channelTurnOnEventIndex in RMON.
Turn off event index is	Value of this object identifies the event that is configured to turn the associated channelDataControl from on to off when the event is generated. Equivalent to channelTurnOffEventIndex in RMON.
Description:	Comment describing this channel.

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
rmon alarm	Sets an alarm on any MIB object.

Command	Description
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.
show rmon	Displays the current RMON agent status on the router.

show rmon history

To display the contents of the router's RMON history table, use the **show rmon history** command in Exec mode.

show rmon history

Syntax Description

This command has no arguments or keywords.

Command Mode

Exec

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

For additional information, refer to the RMON MIB described in RFC 1757.

You must have first enabled RMON on the interface, and configured RMON alarms and events to display alarm information with the **show rmon history** command.

This command is available on the Cisco 2500 series and Cisco AS5200 series only.

Examples

The following is sample output from the **show rmon history** command:

```
Router# show rmon history

Entry 1 is active, and owned by manager1
 Monitors ifEntry.1.1 every 30 seconds
 Requested # of time intervals, ie buckets, is 5
 Granted # of time intervals, ie buckets, is 5
  Sample # 14 began measuring at 00:11:00
   Received 38346 octets, 216 packets,
   0 broadcast and 80 multicast packets,
   0 undersized and 0 oversized packets,
   0 fragments and 0 jabbers,
   0 CRC alignment errors and 0 collisions.
   # of dropped packet events is 0
   Network utilization is estimated at 10
```

Table 96 describes the significant fields shown in the display.

Table 96 show rmon history Field Descriptions

Field	Description
Entry 1 is active, and owned by manager1	Unique index of the history entry, its current state, and the owner as defined in the historyControlTable of RMON.
Monitors ifEntry.1.1	This object identifies the source of the data for which historical data was collected and placed in a media-specific table. Equivalent to historyControlDataSource in RMON.

Table 96 show rmon history Field Descriptions (continued)

Field	Description
every 30 seconds	Interval in seconds over which the data is sampled for each bucket in the part of the media-specific table associated with this historyControlEntry. Equivalent to historyControlInterval in RMON.
Requested # of time intervals, ie buckets, is	Requested number of discrete time intervals over which data is to be saved in the part of the media-specific table associated with this historyControlEntry. Equivalent to historyControlBucketsRequested in RMON.
Granted # of time intervals, ie buckets, is	Actual number of discrete time intervals over which data is to be saved in the part of the media-specific table associated with this historyControlEntry. Equivalent to historyControlBucketsGranted in RMON.
Sample # 14 began measuring at	Time at the start of the interval over which this sample was measured.
Received 38346 octets	Total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). Equivalent to etherHistoryOctets in RMON.
x packets	Number of packets (including bad packets) received during this sampling interval. Equivalent to etherHistoryPkts in RMON.
x broadcast	Number of good packets received during this sampling interval that were directed to the broadcast address. Equivalent to etherHistoryBroadcastPkts in RMON.
x multicast packets	Number of good packets received during this sampling interval that were directed to a multicast address. Equivalent to etherHistoryMulticastPkts in RMON.
x undersized	Number of packets received during this sampling interval that were fewer than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed. Equivalent to etherHistoryUndersizedPkts in RMON.
x oversized packets	Number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed. Equivalent to etherHistoryOversizePkts in RMON.
x fragments	Total number of packets received during this sampling interval that were fewer than 64 octets in length (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). Equivalent to etherHistoryFragments in RMON.

Table 96 show rmon history Field Descriptions (continued)

Field	Description
x jabbers	Number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). Equivalent to etherHistoryJabbers in RMON.
x CRC alignment errors	Number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) from 64 to 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). Equivalent to etherHistoryCRCAlignErrors in RMON.
x collisions	Best estimate of the total number of collisions on this Ethernet segment during this sampling interval. Equivalent to etherHistoryCollisions in RMON.
# of dropped packet events is	Total number of events in which packets were dropped by the operation because of resources during this sampling interval. Note that this number is not necessarily the number of packets dropped, it is just the number of times this condition has been detected. Equivalent to etherHistoryDropEvents in RMON.
Network utilization is estimated at	Best estimate of the mean physical-layer network usage on this interface during this sampling interval, in hundredths of a percent. Equivalent to etherHistoryUtilization in RMON.

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
rmon alarm	Sets an alarm on any MIB object.
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.
show rmon	Displays the current RMON agent status on the router.

show rmon hosts

To display the contents of the router's RMON hosts table, use the **show rmon hosts** command in Exec mode.

show rmon hosts

Syntax Description

This command has no arguments or keywords.

Command Mode

Exec

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

You must have first enabled RMON on the interface, and configured RMON alarms and events to display alarm information with the **show rmon hosts** command.

This command is available on the Cisco 2500 series and Cisco AS5200 series only.

For additional information, refer to the RMON MIB described in RFC 1757.

Examples

The following is sample output from the **show rmon hosts** command:

```
Router# show rmon hosts

Host Control Entry 1 is active, and owned by manager1
 Monitors host ifEntry.1.1
 Table size is 51, last time an entry was deleted was 00:00:00
  Creation Order number is 1
   Physical address is 0000.0c02.5808
   Packets: rcvd 6963, transmitted 7041
   Octets: rcvd 784062, transmitted 858530
   # of packets transmitted: broadcast 28, multicast 48
   # of bad packets transmitted is 0
```

Table 97 describes the significant fields shown in the display.

Table 97 show rmon hosts Field Descriptions

Field	Description
Host Control Entry 1 is active, and owned by manager1	Unique index of the host entry, its current state, and the owner as defined in the hostControlTable of RMON.
Monitors host ifEntry.1.1	This object identifies the source of the data for this instance of the host function. Equivalent to hostControlDataSource in RMON.

Table 97 show rmon hosts Field Descriptions (continued)

Field	Description
Table size is	Number of hostEntries in the hostTable and the hostTimeTable associated with this hostControlEntry. Equivalent to hostControlTableSize in RMON.
last time an entry was deleted was	Time when the last entry was deleted from the hostTable.
Creation Order number is	Index that defines the relative ordering of the creation time of hosts captured for a particular hostControlEntry. Equivalent to hostCreationOrder in RMON.
Physical address is	Physical address of this host. Equivalent to hostAddress in RMON.
Packets: rcvd	Number of good packets transmitted to this address. Equivalent to hostInPkts in RMON.
transmitted	Number of packets, including bad packets transmitted by this address. Equivalent to hostOutPkts in RMON.
Octets: rcvd	Number of octets transmitted to this address since it was added to the hostTable (excluding framing bits but including FCS octets), except for those octets in bad packets. Equivalent to hostInOctets in RMON.
transmitted	Number of octets transmitted by this address since it was added to the hostTable (excluding framing bits but including FCS octets), including those octets in bad packets. Equivalent to hostOutOctets in RMON.
# of packets transmitted:	Number of good packets transmitted by this address that were broadcast or multicast.
# of bad packets transmitted is	Number of bad packets transmitted by this address.

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
rmon alarm	Sets an alarm on any MIB object.
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.
show rmon	Displays the current RMON agent status on the router.

show rmon matrix

To display the contents of the router's RMON matrix table, use the **show rmon matrix** command in Exec mode.

show rmon matrix

Syntax Description

This command has no arguments or keywords.

Command Mode

Exec

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

You must have first enabled RMON on the interface, and configured RMON alarms and events to display alarm information with the **show rmon matrix** command.

This command is available on the Cisco 2500 series and Cisco AS5200 series only.

For additional information, refer to the RMON MIB described in RFC 1757.

Examples

The following is sample output from the **show rmon matrix** command:

```
Router# show rmon matrix

Matrix 1 is active, and owned by manager1
 Monitors ifEntry.1.1
 Table size is 451, last time an entry was deleted was at 00:00:00
```

Table 98 describes the significant fields shown in the display.

Table 98 show rmon matrix Field Descriptions

Field	Description
Matrix 1 is active, and owned by manager1	Unique index of the matrix entry, its current state, and the owner as defined in the matrixControlTable of RMON.
Monitors ifEntry.1.1	This object identifies the source of the data for this instance of the matrix function. Equivalent to matrixControlDataSource in RMON.
Table size is 451, last time an entry was deleted was at	Size of the matrix table and the time that the last entry was deleted.

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
rmon alarm	Sets an alarm on any MIB object.

Command	Description
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.
show rmon	Displays the current RMON agent status on the router.

show rmon statistics

To display the contents of the router's RMON statistics table, use the **show rmon statistics** command in Exec mode.

show rmon statistics

Syntax Description

This command has no arguments or keywords.

Command Mode

Exec

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

For additional information, refer to the RMON MIB described in RFC 1757.

You must have first enabled RMON on the interface, and configured RMON alarms and events to display alarm information with the **show rmon statistics** command.

This command is available on the Cisco 2500 series and Cisco AS5200 series only.

Examples

The following is sample output from the **show rmon statistics** command:

```
Router# show rmon statistics

Interface 1 is active, and owned by config
 Monitors ifEntry.1.1 which has
 Received 60739740 octets, 201157 packets,
 1721 broadcast and 9185 multicast packets,
 0 undersized and 0 oversized packets,
 0 fragments and 0 jabbers,
 0 CRC alignment errors and 32 collisions.
 # of dropped packet events (due to lack of resources): 511
 # of packets received of length (in octets):
  64: 92955, 65-127: 14204, 128-255: 1116,
  256-511: 4479, 512-1023: 85856, 1024-1518:2547
```

Table 99 describes the significant fields shown in the display.

Table 99 show rmon statistics Field Descriptions

Field	Description
Interface 1 is active, and owned by config	Unique index of the statistics entry, its current state, and the owner as defined in the etherStatsTable of RMON.
Monitors ifEntry.1.1	This object identifies the source of the data that this etherStats entry is configured to analyze. Equivalent to etherStatsDataSource in RMON.

Table 99 show rmon statistics Field Descriptions (continued)

Field	Description
Received 60739740 octets	Total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). Equivalent to etherStatsOctets in RMON.
x packets	Number of packets (including bad packets) received. Equivalent to etherStatsPkts in RMON.
x broadcast	Number of good packets received that were directed to the broadcast address. Equivalent to etherStatsBroadcastPkts in RMON.
x multicast packets	Number of good packets received that were directed to a multicast address. Equivalent to etherStatsMulticastPkts in RMON.
x undersized	Number of packets received that were fewer than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed. Equivalent to etherStatsUndersizedPkts in RMON.
x oversized packets	Number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed. Equivalent to etherStatsOversizePkts in RMON.
x fragments	Total number of packets received that were fewer than 64 octets in length (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). Equivalent to etherStatsFragments in RMON.
x jabbers	Number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). Equivalent to etherStatsJabbers in RMON.
x CRC alignment errors	Number of packets received that had a length (excluding framing bits but including FCS octets) from 64 to 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). Equivalent to etherStatsCRCAlignErrors in RMON.
x collisions	Best estimate of the total number of collisions on this Ethernet segment. Equivalent to etherHistoryCollisions in RMON.

Table 99 show rmon statistics Field Descriptions (continued)

Field	Description
# of dropped packet events (due to lack of resources):	Total number of events in which packets were dropped by the operation because of a lack of resources. Note that this number is not necessarily the number of packets dropped, it is just the number of times this condition has been detected. Equivalent to etherStatsDropEvents in RMON.
# of packets received of length (in octets):	Separates the received packets (good and bad) by packet size in the given ranges (64, 65 to 127,128 to 255, 256 to 511, 512 to 1023, 1024 to 1516).

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
rmon alarm	Sets an alarm on any MIB object.
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.
show rmon	Displays the current RMON agent status on the router.

show rmon topn

To display the contents of the router's RMON Top-N host table, use the **show rmon topn** command in Exec mode.

show rmon topn

Syntax Description

This command has no arguments or keywords.

Command Mode

Exec

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

For additional information, refer to the RMON MIB described in RFC 1757.

You must have first enabled RMON on the interface, and configured RMON events to display alarm information with the **show rmon events** command.

This command is available on the Cisco 2500 series and Cisco AS5200 series only.

Examples

The following is sample output from the **show rmon topn** command:

```
Router# show rmon topn

Host Entry 1 of report 1 is active, owned by manager1
 The rate of change is based on hostTopNInPkts
 This report was last started at 00:00:00
 Time remaining in this report is 0 out of 0
 Hosts physical address is 00ad.beef.002b
 Requested # of hosts: 10, # of hosts granted: 10
Report # 1 of Top N hosts entry 1 is recording
Host 0000.0c02.5808 at a rate of 12
```

Table 100 describes the significant fields shown in the display.

Table 100 show rmon topn Field Descriptions

Field	Description
Host Entry 1 of report 1 is active, owned by manager1	Unique index of the hostTopN entry, its current state, and the owner as defined in the hostTopNControlTable of RMON.
The rate of change is based on hostTopNInPkts	Variable for each host that the hostTopNRate variable is based on.
This report was last started at	Time the report was started.

Table 100 show rmon topn Field Descriptions (continued)

Field	Description
Time remaining in this report is	Number of seconds left in the report currently being collected. Equivalent to hostTopNTimeRemaining in RMON.
out of	Number of seconds that this report has collected during the last sampling interval, or if this report is currently being collected, the number of seconds that this report is being collected during this sampling interval. Equivalent to hostTopNDuration in RMON.
Hosts physical address is	Host address.
Requested # of hosts:	Maximum number of hosts requested for the Top-N table. Equivalent to hostTopNRequestedSize in RMON.
# of hosts granted:	Maximum number of hosts granted for the Top-N table.Eqivalent to hostTopNGrantedSiz in RMON.
Report # 1 of Top N hosts entry 1 is recording	Report number and entry.
Host 0000.0c02.5808 at a rate of	Physical address of the host, and the amount of change in the selected variable during this sampling interval. Equivalent to hostTopNAddress and hostTopNRate in RMON.

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
rmon alarm	Sets an alarm on any MIB object.
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.
show rmon	Displays the current RMON agent status on the router.

show rom-monitor

To show both the ReadOnly and the Upgrade ROMmon image versions, as well as which ROMmon image is running on the Cisco 7200 VXR or Cisco 7301 router, use the **show rom-monitor** command in privileged Exec mode.

show rom-monitor

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Mode

Privileged Exec

Command History

Release	Modification
12.0(28)S	This command was introduced on the Cisco 7200 VXR router.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T and supported on the Cisco 7200 VXR router and Cisco 7301 router.
12.3(9)	This command was integrated into Cisco IOS Release 12.3(9) and supported on the Cisco 7200 VXR router and Cisco 7301 router.

Usage Guidelines

Use the **show rom-monitor** command when you are in Cisco IOS. Use the **showmon** command when you are in ROMmon mode.

Examples

The following example, applicable to both the Cisco 7200 VXR and Cisco 7301 routers, uses the **show rom-monitor** command in Cisco IOS to display both ROMmon images and to verify that the Upgrade ROMmon image is running:

```
Router> show rom-monitor
ReadOnly ROMMON version:

System Bootstrap, Version 12.2(20031011:151758)
Copyright (c) 2004 by Cisco Systems, Inc.

Upgrade ROMMON version:

System Bootstrap, Version 12.2(20031011:151758)
Copyright (c) 2004 by Cisco Systems, Inc.

Currently running ROMMON from Upgrade region
ROMMON from Upgrade region is selected for next boot
```

Related Commands

Command	Description
showmon	Shows both the ReadOnly and the Upgrade ROMmon image versions when you are in ROMmon mode, as well as which ROMmon image is running.

show rtr application

To display global information about the Service Assurance Agent (SAA) feature, use the **show rtr application** command in Exec mode.

show rtr application [**tabular** | **full**]

Syntax Description

tabular	(Optional) Displays information in a column format reducing the number of screens required to display the information.
full	(Optional) Displays all information using identifiers next to each displayed value. This is the default.

Defaults

Full format

Command Mode

Exec

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use the **show rtr application** command to display information such as supported operation types and supported protocols.

Examples

The following is sample output from the **show rtr application** command in full format:

```
Router#s how rtr application

        Response Time Reporter
Version: 2.2.0 Round Trip Time MIB
Max Packet Data Size (ARR and Data): 16384
Time of Last Change in Whole RTR: 03:34:44.000 UTC Sun Feb 11 2001
System Max Number of Entries: 2000

Number of Entries configured:5
    Number of active Entries:5
   Number of pending Entries:0
  Number of inactive Entries:0
         Supported Operation Types
Type of Operation to Perform:  echo
Type of Operation to Perform:  pathEcho
Type of Operation to Perform:  udpEcho
Type of Operation to Perform:  tcpConnect
Type of Operation to Perform:  http
Type of Operation to Perform:  dns
Type of Operation to Perform:  jitter
Type of Operation to Perform:  dlsw
Type of Operation to Perform:  dhcp
Type of Operation to Perform:  ftp
```

```
        Supported Protocols
Protocol Type: ipIcmpEcho
Protocol Type: ipUdpEchoAppl
Protocol Type: snaRUEcho
Protocol Type: snaLU0EchoAppl
Protocol Type: snaLU2EchoAppl
Protocol Type: ipTcpConn
Protocol Type: httpAppl
Protocol Type: dnsAppl
Protocol Type: jitterAppl
Protocol Type: dlsw
Protocol Type: dhcp
Protocol Type: ftpAppl

Number of configurable probe is 490
```

Related Commands

Command	Description
show rtr configuration	Displays configuration values including all defaults for all SAA operations or the specified operation.

show rtr authentication

To display Service Assurance Agent (SAA) Response Time Reporter (RTR) authentication information, use the **show rtr authentication** command in Exec mode.

show rtr authentication

Syntax Description

This command has no arguments or keywords.

Command Mode

Exec

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

Use the **show rtr authentication** command to display information such as supported operation types and supported protocols.

Examples

The following is sample output from the **show rtr authentication** command:

```
Router# show rtr authentication

RTR control message uses MD5 authentication, key chain name is: rtr
```

Related Commands

Command	Description
show rtr configuration	Displays configuration values for RTR operations (probes).

show rtr collection-statistics

To display statistical errors for all Service Assurance Agent (SAA) operations or a specified operation, use the **show rtr collection-statistics** command in Exec mode.

show rtr collection-statistics [*operation-number*] [**tabular** | **full**]

Syntax Description

operation-number	(Optional) Number of the SAA operation to display.
tabular	(Optional) Display information in a column format reducing the number of screens required to display the information.
full	(Optional) Display all information using identifiers next to each displayed value. This is the default.

Defaults

Full format for all operations. Shows statistics for the past two hours.

Command Mode

Exec

Command History

Release	Modification
11.2	This command was introduced.
12.0(5)T	The output for this command was expanded to show information for Jitter operations.
12.1(1)T	The output for this command was expanded to show information for the FTP operation and for One Way Delay Jitter operations.
12.2(11)T	The SAA Engine II was implemented. The maximum number of operations was increased from 500 to 2000.

Usage Guidelines

Use the **show rtr collection-statistics** command to display information such as the number of failed operations and the failure reason. You can also use the **show rtr distribution-statistics** and **show rtr totals-statistics** commands to display additional statistical information.

This command shows information collected over the past two hours, unless you specify a different amount of time using the **hours-of-statistics-kept** command.

For One Way Delay Jitter operations, the clocks on each device must be synchronized using NTP (or GPS systems). If the clocks are not synchronized, one-way measurements are discarded. (If the sum of the source to destination (SD) and the destination to source (DS) values is not within 10 percent of the round trip time, the one-way measurement values are assumed to be faulty, and are discarded.)

Examples

The following is sample output from the **show rtr collection-statistics** command in full format.

```
Router# show rtr collection-statistics 1

        Collected Statistics
Entry Number: 1
```

```
Start Time Index: *17:15:41.000 UTC Thu May 16 1996
Path Index: 1
Hop in Path Index: 1
Number of Failed Operations due to a Disconnect: 0
Number of Failed Operations due to a Timeout: 0
Number of Failed Operations due to a Busy: 0
Number of Failed Operations due to a No Connection: 0
Number of Failed Operations due to an Internal Error: 0
Number of Failed Operations due to a Sequence Error: 0
Number of Failed Operations due to a Verify Error: 0
Target Address: 172.16.1.176
```

The following example verifies that the statistics are being collected for an HTTP operation:

```
router# show rtr collection-statistics 2

        Collected Statistics

Entry Number:2
HTTP URL:http://172.20.150.200
Start Time:*00:01:16.000 UTC Mon Mar 1 1993

             Comps:1              RTTMin:343
             OvrTh:0              RTTMax:343
        DNSTimeOut:0              RTTSum:343
        TCPTimeOut:0             RTTSum2:117649
        TraTimeOut:0              DNSRTT:0
          DNSError:0           TCPConRTT:13
         HTTPError:0            TransRTT:330
          IntError:0            MesgSize:1771
             Busies:0
```

The following is sample output from the **show rtr collection-statistics** command, where operation 1 is a Jitter operation which includes One Way reporting Values:

```
Router# show rtr collection-statistics

Collected Statistics

Entry Number: 1
Target Address: 5.0.0.1, Port Number:99
Start Time: 11:12:03.000 UTC Thu Jul 1 1999
RTT Values:
NumOfRTT: 600  RTTSum: 3789  RTTSum2: 138665
Packet Loss Values:
PacketLossSD: 0  PacketLossDS: 0
PacketOutOfSequence: 0  PacketMIA: 0  PacketLateArrival: 0
InternalError: 0  Busies: 0
Jitter Values:
MinOfPositivesSD: 1   MaxOfPositivesSD: 2
NumOfPositivesSD: 26  SumOfPositivesSD: 31   Sum2PositivesSD: 41
MinOfNegativesSD: 1   MaxOfNegativesSD: 4
NumOfNegativesSD: 56  SumOfNegativesSD: 73   Sum2NegativesSD: 133
MinOfPositivesDS: 1   MaxOfPositivesDS: 338
NumOfPositivesDS: 58  SumOfPositivesDS: 409  Sum2PositivesDS: 114347
MinOfNegativesDS: 1   MaxOfNegativesDS: 338
NumOfNegativesDS: 48  SumOfNegativesDS: 396  Sum2NegativesDS: 114332
One Way Values:
NumOfOW: 440
OWMinSD: 2  OWMaxSD: 6    OWSumSD: 1273  OWSum2SD: 4021
OWMinDS: 2  OWMaxDS: 341  OWSumDS: 1643  OWSum2DS: 120295
```

The values shown indicate the aggregated values for the current hour. RTT stands for Round-Trip-Time. SD stands for Source-to-Destination. DS stands for Destination-to-Source. OW stands for One Way. Table 101 describes the significant fields shown in this output.

Table 101 show rtr collection-statistics Field Descriptions

Field	Description
NumOfRTT	The number of successful round trips.
RTTSum	The sum of those round trip values (in milliseconds).
RTTSum2	The sum of squares of those round trip values (in milliseconds).
PacketLossSD	The number of packets lost from source to destination.
PacketLossDS	The number of packets lost from destination to source.
PacketOutOfSequence	The number of packets returned out of order.
PacketMIA	The number of packets lost where the direction (SD/DS) cannot be determined.
PacketLateArrival	The number of packets that arrived after the timeout.
InternalError	The number of times an operation could not be started due to other internal failures.
Busies	The number of times this operation could not be started because the previously scheduled run was not finished.
MinOfPositivesSD MaxOfPositivesSD	The minimum and maximum positive jitter values from source to destination, in milliseconds.
NumOfPositivesSD	The number of jitter values from source to destination that are positive (i.e., network latency increases for two consecutive test packets).
SumOfPositivesSD	The sum of those positive values (in milliseconds).
Sum2PositivesSD	The sum of squares of those positive values.
MinOfNegativesSD MaxOfNegativesSD	The minimum and maximum negative jitter values from source to destination. The absolute value is given.
NumOfNegativesSD	The number of jitter values from source to destination that are negative (i.e., network latency decreases for two consecutive test packets).
SumOfNegativesSD	The sum of those values.
Sum2NegativesSD	The sum of the squares of those values.
One Way Values	Amount of time it took the packet to travel from the source router to the target router or from the target router to the source router.
NumOfOW	Number of successful one-way time measurements.
OWMinSD	Minimum time from the source to the destination.

Table 101 show rtr collection-statistics Field Descriptions (continued)

Field	Description
OWMaxSD	Maximum time from the source to the destination.
OWSumSD	Sum of the OWMinSD and OWMaxSD values.
OWSum2SD	Sum of the squares of the OWMinSD and OWMaxSD values.

The DS values show the same information as above for Destination-to-Source Jitter values.

Related Commands

Command	Description
show ntp status	Displays the status of the Network Time Protocol configuration on your system.
show rtr configuration	Displays configuration values including all defaults for all SA Agent operations or the specified operation.
show rtr distributions-statistics	Displays statistic distribution information (captured response times) for all SAA operations or the specified operation.
show rtr totals-statistics	Displays the total statistical values (accumulation of error counts and completions) for all SAA operations or the specified operation.

show rtr configuration

To display configuration values including all defaults for all Service Assurance Agent (SAA) operations or the specified operation, use the **show rtr configuration** command in Exec mode.

show rtr configuration [*operation*] [**tabular** | **full**]

Syntax Description

operation	(Optional) Number of the SAA operation to display.
tabular	(Optional) Display information in a column format reducing the number of screens required to display the information.
full	(Optional) Display all information using identifiers next to each displayed value. This is the default.

Defaults

Full format for all operations

Command Mode

Exec

Command History

Release	Modification
11.2	This command was introduced.

Examples

The following is sample output from the **show rtr configuration** command in full format:

```
Router# show rtr configuration 1

        Complete Configuration Table (includes defaults)
Entry Number: 1
Owner: "Sample Owner"
Tag: "Sample Tag Group"
Type of Operation to Perform: echo
Reaction and History Threshold (milliseconds): 5000
Operation Frequency (seconds): 60
Operation Timeout (milliseconds): 5000
Verify Data: FALSE
Status of Entry (SNMP RowStatus): active
Protocol Type: ipIcmpEcho
Target Address: 172.16.1.176
Request Size (ARR data portion): 1
Response Size (ARR data portion): 1
Life (seconds): 3600
Next Start Time: Start Time already passed
Entry Ageout (seconds): 3600
Connection Loss Reaction Enabled: FALSE
Timeout Reaction Enabled: FALSE
Threshold Reaction Type: never
Threshold Falling (milliseconds): 3000
Threshold Count: 5
Threshold Count2: 5
Reaction Type: none
Number of Statistic Hours kept: 2
```

```
Number of Statistic Paths kept: 1
Number of Statistic Hops kept: 1
Number of Statistic Distribution Buckets kept: 1
Number of Statistic Distribution Intervals (milliseconds): 20
Number of History Lives kept: 0
Number of History Buckets kept: 50
Number of History Samples kept: 1
History Filter Type: none
```

The following example verifies the configuration of an HTTP operation:

```
Router# show rtr configuration

        Complete Configuration Table (includes defaults)
Entry Number:3
Owner:Joe
Tag:AppleTree
Type of Operation to Perform:http
Reaction and History Threshold (milliseconds):5000
Operation Frequency (seconds):60
Operation Timeout (milliseconds):5000
Verify Data:FALSE
Status of Entry (SNMP RowStatus):active
Protocol Type:httpAppl
Target Address:
Source Address:0.0.0.0
Target Port:0
Source Port:0
Request Size (ARR data portion):1
Response Size (ARR data portion):1
Control Packets:enabled
Loose Source Routing:disabled
LSR Path:
Type of Service Parameters:0x0
HTTP Operation:get
HTTP Server Version:1.0
URL:http://www.cisco.com
Cache Control:enabled
Life (seconds):3600
Next Scheduled Start Time:Start Time already passed
Entry Ageout:never
Connection Loss Reaction Enabled:FALSE
Timeout Reaction Enabled:FALSE
Threshold Reaction Type:never
Threshold Falling (milliseconds):3000
Threshold Count:5
Threshold Count2:5
Reaction Type:none
Number of Statistic Hours kept:2
Number of Statistic Paths kept:1
Number of Statistic Hops kept:1
Number of Statistic Distribution Buckets kept:1
Statistic Distribution Interval (milliseconds):20
Number of History Lives kept:0
Number of History Buckets kept:15
Number of History Samples kept:1
History Filter Type:none
```

Related Commands

Command	Description
show rtr application	Displays global information about the SAA feature.
show rtr collection-statistics	Displays statistical errors for all SAA operations or the specified operation.
show rtr distributions-statistics	Displays statistic distribution information (captured response times) for all SAA operations or the specified operation.
show rtr history	Displays history collected for all SAA operations or the specified operation.
show rtr operational-state	Displays the operational state of all SAA operations or the specified operation.
show rtr reaction-trigger	Displays the reaction trigger information for all SAA operations or the specified operation.
show rtr totals-statistics	Displays the total statistical values (accumulation of error counts and completions) for all SAA operations or the specified operation.

show rtr enhanced-history collection-statistics

To display enhanced history statistics for all collected history buckets for the specified Service Assurance Agent (SAA) operation, use the **show rtr enhanced-history distributio-statistics** command in user Exec or privileged Exec mode.

show rtr enhanced-history collection-statistics [*operation-number*]

Syntax Description

operation-number	(Optional) Displays enhanced history distribution statistics for only the specified operation.
dlci	Data link connection identifier of the permanent virtual circuit (PVC) to be monitored.

Command Mode

User Exec

Privileged Exec

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

This command displays data for each bucket of enhanced history data shown individually (one after the other).

The number of buckets and the collection interval is set using the **enhanced-history interval** *seconds* **buckets** *number-of-buckets* SAA RTR configuration mode command.

For SLM operations, the enhanced history collection interval is set at 900 seconds and the number of buckets is set at 100. Because the enhanced history aggregationinterval is fixed at 900 seconds, the optional **interval** keyword available for this command will not work for SLM operations.

Examples

The output of this command will vary depending on the operation type. The following examples show output for various SAA operations.

Output for SLM Controller Operation

```
Router# show rtr configuration 1 | include Type
Type of operation to perform: slm controller
Reaction Type: None

Router# show running-config | begin rtr
.
.
.
```

```
rtr 1
 type slm controller T1 0
 enhanced-history interval 900 buckets 100
rtr schedule 1 start-time now life forever
.
.
.
Router# show rtr enhanced-history collection-statistics 1
Entry number: 1
Aggregation Interval: 900

Bucket Index: 1
Aggregation start time 00:15:00.003 UTC Thur May 1 2003
Target Address:
Number of failed operations due to a Disconnect: 0
Number of failed operations due to a Timeout: 0
Number of failed operations due to a Busy: 0
Number of failed operations due to a No Connection: 0
Number of failed operations due to an Internal Error: 0
Number of failed operations due to a Sequence Error: 0
Number of failed operations due to a Verify Error: 0


  Ds1StatRxLineStatus:  16385
  Ds1StatRxBPVs:  0,              Ds1StatRxCrcFrameErrors:  0
  Ds1StatRxErrSecs:  0,           Ds1StatRxSevereErrSecs:  0
  Ds1StatRxUnavailSecs:  0,       Ds1StatRxBurstyErrSecs:  0

Sample Index = 1

Bucket Index: 2
 .
 .
 .
```

Table 102 describes the significant fields shown in the display.

Table 102 show rtr enhanced-history Field Descriptions for SLM Controller Operations

Field	Description
Aggregation Interval:	The number of seconds the operation runs for each enhanced history bucket. For example, a value of 900 indicates that statistics were gathered for 15 minutes before the next bucket was created.
Bucket Index:	The number identifying the collection bucket. The number of buckets is set using the **enhanced-history** SAA RTR configuration command.
Ds1StatRx	DS1 and E1 Received Statistics—The Ds1StatRx prefix is used for DS1 and E1 interfaces. DS1 and E1 interfaces are physical interfaces that run at a medium speed (for example, 1544 Kbps for DS1 interfaces). “Rx” indicates “received.”

Table 102 show rtr enhanced-history Field Descriptions for SLM Controller Operations (continued)

Field	Description
Ds1StatRxLineStatus:	Line Status—This variable indicates the Line Status of the interface. The dsx1LineStatus is a bit map represented as a sum, therefore, it can represent multiple conditions, like Excess Zeros and B8ZS detect, simultaneously. For example, the outOfFrame condition is implied by an outOfSignal condition. Possible values include: • 2 — yellowAlarm • 8 — blueAlarm • 32 — outOfFrame • 64 — outOfSignal • 8192 — excessZeros • 16384 — b8zsDetect
Ds1StatRxBPVs:	Bi-Polar Violations—The total number of Bipolar Violations (BPVs) received on the interface.
Ds1StatRxCrcFrameErrors:	CRC or Frame Errors—he total number of Cyclic Redundancy Check (CRC) Errors (with ESF framing) or Frame Errors (with D4 framing) received on the interface.
Ds1StatRxErrSecs:	Errored Seconds—The total number of Errored Seconds that have occurred on the interface. This includes both Line Errored and Path Errored Seconds.
Ds1StatRxSevereErrSecs:	Severely Errored Seconds—The total number of Severely Errored Seconds that have occurred on the interface. This includes both Line Severely Errored Seconds and Path Severely Errored Seconds.
Ds1StatRxUnavailSecs:	Unavailable Seconds—The total number of Unavailable Seconds that have occurred on the interface.
Ds1StatRxBurstyErrSecs:	Type B Errored Seconds—The total number of Type B (Bursty) Errored Seconds that have occurred on the interface.
Ds1StatRxREBEs:	E1 Remote-End Block Errors—The total number of Remote-End Block Error (REBE) Events received on an E1 interface. (This data does not appear for DS1 interfaces.)

Output for SLM Frame Relay Operation

```
Router# show rtr configuration 2 | include Type
Type of operation to perform: Slm Frame-relay Interface
Reaction Type: None
Router#
Router# show rtr ennhanced-history collection-statistics 2
Entry number: 2
Aggregation Interval: 900

Bucket Index: 1
Aggregation start time 00:15:00.003 UTC Mon Mar 1 1993
```

```
Target Address:
Number of failed operations due to a Disconnect: 0
Number of failed operations due to a Timeout: 0
Number of failed operations due to a Busy: 0
Number of failed operations due to a No Connection: 0
Number of failed operations due to an Internal Error: 0
Number of failed operations due to a Sequence Error: 0
Number of failed operations due to a Verify Error: 0

LinkState :1
Tx Total Frames:  24                      Rx Total Frames:  24
Tx Total Octets:  312                     Rx Total Octets:  344
Tx FCSAlignErrors:  0                     Rx FCSAlignErrors:  0
Tx Aborted Frames:  0                     Rx Aborted Frames:  0
Tx Long Frames:  0                        Rx Long Frames:  0
Tx Short Frames:  0                       Rx Short Frames:  0
Tx MaxThroughput:  88                     Rx MaxThroughput:  152
Tx MaxUtilization:  0                     Rx MaxUtilization:  0
Tx MaxFramesSec:  1                       Rx MaxFramesSec:  1
UnavailSecs:  0                           Drop Events:  0
Tx OverFlowOctets:  0                     Rx OverFlowOctets:  0

Tx Burst Percent1(sec):  238              Rx Burst Percent1(sec): 238
Tx Burst Percent2(sec):  0                Rx Burst Percent2(sec): 0
Tx Burst Percent3(sec):  0                Rx Burst Percent3(sec): 0
Tx Burst Percent4(sec):  0                Rx Burst Percent4(sec): 0
Tx Burst Percent5(sec):  0                Rx Burst Percent5(sec): 0

Sample Index = 1

Bucket Index: 2
 .
 .
 .
```

Table 103 describes the significant fields shown in the display. In the output “Tx” indicates “transmitted,” “Rx” indicates “received.”

Table 103 show rtr enhanced-history collection-statistics Field Descriptions for SLM Frame Relay Operations

Field	Description
LinkState	The Link State of the Frame Relay access channel being monitored. The link state is determined by the presence of LMI messages on the user and network side of the line. The link state can take the following values: • up(1)—Both sides of the access channel are up. • networkDown(2)—The network side of the circuit has not responded to at least frDlcmiErrorThreshold Status Enquiry messages. • userDown(3)—The user side of the access channel has not sent a Status Enquiry LMI message in FrConfigPollingTimeoutInterval (T391) seconds. • down(4)—Both sides of the access channel have been down over some portion of the sampling interval. • spoofNetworkUp(5)—The agent has been spoofing for the user over some portion of the sampling interval while the network side of the access channel has been up over the entire sampling interval. • spoofNetworkDown(6)— The agent has been spoofing for the user over some portion of the sampling interval while the network side of the access channel has been down over the entire sampling interval.
Tx Total Frames:	The total number of frames (including errored frames) transmitted by the interface. Aborted frames are not included in this count. (MIB variable: FrStatTxFrames)
Rx Total Frames:	The total number of non-errored frames received by the interface. Aborted frames are not included. (MIB variable: FrStatRxFrames)
Tx Total Octets:	The total number of octets transmitted in frames from the interface (excluding framing bits but including FCS octets). Octets in errored and aborted frames are included in this count. (MIB variable: FrStatTxOctets)
Rx Total Octets:	The total number of octets received by the interface in non-errored frames (excluding framing bits but including FCS octets). Octets in errored and aborted frames are included in this count. (MIB variable: FrStatRxOctets)

Table 103 show rtr enhanced-history collection-statistics Field Descriptions for SLM Frame Relay Operations (continued)

Field	Description
Tx FCSAlignErrors:	The total number of frames transmitted by the interface that had a length (excluding framing bits, but including FCS octets) of at least (5) octets, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Agents that cannot count this transmit-side object will return a value of zero. (MIB variable: FrStatTxFcsAlignErrors)
Rx FCSAlignErrors:	The total number of frames received by the interface that had a length (excluding framing bits, but including FCS octets) of at least (5) octets, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). (MIB variable: FrStatRxFcsAlignErrors)
Tx Burst Percent1(sec):	The number of one second intervals where the transmitted throughput (t) is greater than or equal to zero and less than or equal to BurstLimit 1 (0 <= t <= BurstLimit1). BurstLimit1 is defined as a percentage of the CircuitBurstNominalRate in the RTTMON MIB. Note: The burst parameters used in this definition are defined in the CircuitConfigTable of the RTTMON MIB.

show rtr enhanced-history distribution-statistics

To display enhanced history distribution statistics for Service Assurance Agent (SAA) operations in tabular format, use the **show rtr enhanced-history distribution-statistics** command in user Exec or privileged Exec mode.

show rtr enhanced-history distribution-statistics [*operation-number*] [**interval** *seconds*]

Syntax Description

operation-number	(Optional) Displays enhanced history distribution statistics for only the specified operation.
interval *seconds*	(Optional) Specifies a distribution interval for the displayed statistics, in seconds. The valid range is from 1 to 3,600 seconds (1 hour). This syntax is not valid for SLM operations. The default is 900 seconds.

Defaults

The default distribution interval is 900 seconds.

Command Mode

User Exec

Privileged Exec

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

The distribution statistics consist of the following:

- The sum of completion times (used to calculate the mean)
- The sum of the completion times squared (used to calculate standard deviation)
- The maximum and minimum completion times
- The number of completed attempts

You can also use the **show rtr enhanced-history collection-statistics** and **show rtr enhanced-history totals-statistics** commands to display additional statistical information.

If the character 'n' appears in your output and not all fields are displayed, you should increase the screen width for your CLI display (for example, using the **width** line configuration command).

Examples

The following is sample output from the **show rtr enhanced-history distribution-statistics** command for an SLM Frame Relay Circuit (Slm Frame-relay Pvc) operation. The fields are defined at the beginning of the output for the command. RTT means round-trip time.

```
Router# show rtr configuration 3 | include Type
Type of operation to perform: Slm Frame-relay Pvc
Reaction Type: None

Router# show rtr enhanced-history distribution-statistics 3
```

```
Point by point Enhanced History
Entry    = Entry Number
Int      = Aggregation Interval (seconds)
BucI     = Bucket Index
StartT   = Aggregation Start Time
Pth      = Path index
Hop      = Hop in path index
Comps    = Operations completed
OvrTh    = Operations completed over thresholds
SumCmp   = Sum of RTT (milliseconds)
SumCmp2L = Sum of RTT squared low 32 bits (milliseconds)
SumCmp2H = Sum of RTT squared high 32 bits (milliseconds)
TMax     = RTT maximum (milliseconds)
TMin     = RTT minimum (milliseconds)

Entry Int BucI StartT    Pth Hop Comps OvrTh SumCmp   SumCmp2L  SumCmp2H   TMax     TMin
3     900 1    257850000 1   1   3     0     43       617        0          15       14
3     900 2    258750002 1   1   3     0     45       677        0          16       14
3     900 3    259650000 1   1   3     0     44       646        0          15       14
3     900 4    260550002 1   1   3     0     42       594        0          15       12
3     900 5    261450003 1   1   3     0     42       590        0          15       13
3     900 6    262350001 1   1   3     0     46       706        0          16       15
3     900 7    263250003 1   1   3     0     46       708        0          16       14
 .
 .
 .
```

Related Commands

Command	Description
rtr	Allows configuration of SAA operations by entering SAA RTR configuration mode for the specified operation number.
show rtr enhanced-history collection-statistics	Displays data for all collected history buckets for the specified SAA operation, with data for each bucket shown individually.

show rtr distributions-statistics

To display statistic distribution information (captured response times) for all Service Assurance Agent (SAA) operations or the specified operation, use the **show rtr distributions-statistics** command in EXEC mode.

show rtr distributions-statistics [*operation*] [**tabular** | **full**]

Syntax Description

operation	(Optional) Number of the SAA operation to display.
tabular	(Optional) Displays information in a column format reducing the number of screens required to display the information. This is the default.
full	(Optional) Displays all information using identifiers next to each displayed value.

Defaults

Tabular format for all operations is displayed.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The distributions statistics consist of the following:

- The sum of completion times (used to calculate the mean)
- The sum of the completions times squared (used to calculate standard deviation)
- The maximum and minimum completion time
- The number of completed attempts

You can also use the **show rtr collection-statistics** and **show rtr totals-statistics** commands to display additional statistical information.

Examples

The following is sample output from the **show rtr distributions-statistics** command in tabular format:

```
Router# show rtr distributions-statistics

        Captured Statistics
        Multiple Lines per Entry
Line 1
Entry    = Entry Number
StartT   = Start Time of Entry (hundredths of seconds)
Pth      = Path Index
Hop      = Hop in Path Index
Dst      = Time Distribution Index
Comps    = Operations Completed
OvrTh    = Operations Completed Over Thresholds
```

```
SumCmp   = Sum of Completion Times (milliseconds)
Line 2
SumCmp2L = Sum of Completion Times Squared Low 32 Bits (milliseconds)
SumCmp2H = Sum of Completion Times Squared High 32 Bits (milliseconds)
TMax     = Completion Time Maximum (milliseconds)
TMin     = Completion Time Minimum (milliseconds)
Entry StartT     Pth Hop Dst Comps      OvrTh      SumCmp
  SumCmp2L   SumCmp2H   TMax       TMin
1     17417068   1   1   1   2          0           128
   8192      0          64         64
```

Related Commands

Command	Description
show rtr collection-statistics	Displays statistical errors for all SAA operations or the specified operation.
show rtr configuration	Displays configuration values including all defaults for all SAA operations or the specified operation.
show rtr totals-statistics	Displays the total statistical values (accumulation of error counts and completions) for all SAA operations or the specified operation.

show rtr history

To display history collected for all Service Assurance Agent (Service Assurance Agent (SAA)) operations or for a specified operation, use the **show rtr history** command in EXEC mode.

show rtr history [*operation-number*] [**tabular** | **full**]

Syntax Description

operation-number	(Optional) Displays history for only the specified operation.
tabular	(Optional) Displays information in a column format reducing the number of screens required to display the information. This is the default.
full	(Optional) Displays all information using identifiers next to each displayed value.

Defaults

Tabular format history for all operations is displayed.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Table 104 lists the Response Return values used in the output of the **show rtr history** command. If the default (**tabular**) format is used, the Response Return description is displayed as a code in the Sense column. If the full format is used, the Response Return is displayed as indicated in the Description column.

Table 104 Response Return (Sense Column) Codes

Code	Description
1	Okay.
2	Disconnected.
3	Over threshold.
4	Timeout.
5	Busy.
6	Not connected.
7	Dropped.
8	Sequence error.
9	Verify error.
10	Application specific.

Examples

The following is sample output from the **show rtr history** command in tabular format:

```
Router# show rtr history

        Point by point History
          Multiple Lines per Entry
Line 1
 Entry    = Entry Number
 LifeI    = Life Index
 BucketI  = Bucket Index
 SampleI  = Sample Index
 SampleT  = Sample Start Time
 CompT    = Completion Time (milliseconds)
 Sense    = Response Return Code
Line 2 has the Target Address
Entry LifeI      BucketI    SampleI    SampleT    CompT      Sense
2     1          1          1          17436548   16          1
  AB 45 A0 16
2     1          2          1          17436551   4           1
  AC 12 7  29
2     1          2          2          17436551   1           1
  AC 12 5  22
2     1          2          3          17436552   4           1
  AB 45 A7 22
2     1          2          4          17436552   4           1
  AB 45 A0 16
```

Related Commands

Command	Description
show rtr configuration	Displays configuration values including all defaults for all SAA operations or the specified operation.

show rtr operational-state

To display the operational state of all Service Assurance Agent (SAA) operations or the specified operation, use the **show rtr operational-state** command in EXEC mode.

show rtr operational-state [*operation-number*]

Syntax Description

operation-number	(Optional) Number of the SAA operation to display.

Defaults

Full format for all operations

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.0(5)T	This command was expanded to show information about Jitter operations.
12.1	The **tabular** and **full** keywords were removed.

Usage Guidelines

Use the **show rtr operational-state** command to determine whether a connection loss, timeout, and over threshold occurred; how much life the operation has left; whether the operation is active; and the completion time. It also displays the results of the latest operation attempt.

Examples

The following example shows sample output from the **show rtr operational-state** command in full format:

```
Router# show rtr operational-state
        Current Operational State
Entry Number:3
Modification Time:*22:15:43.000 UTC Sun Feb 11 2001
Diagnostics Text:
Last Time this Entry was Reset:Never
Number of Octets in use by this Entry:1332
Number of Operations Attempted:2
Current Seconds Left in Life:3511
Operational State of Entry:active
Latest Completion Time (milliseconds):544
Latest Operation Start Time:*22:16:43.000 UTC Sun Feb 11 2001
Latest Oper Sense:ok
Latest Sense Description:200  OK
Total RTT:544
DNS RTT:12
TCP Connection RTT:28
HTTP Transaction RTT:504
HTTP Message Size:9707
```

The following example shows sample output when the specified operation is a Jitter operation:

```
Router# show rtr operational-state 1
        Current Operational State
Entry Number:1
Modification Time:*03:34:44.000 UTC Sun Feb 11 2001
Diagnostics Text:
Last Time this Entry was Reset:Never
Number of Octets in use by this Entry:1382
Number of Operations Attempted:1
Current Seconds Left in Life:3545
Operational State of Entry:active
Latest Operation Start Time:*03:34:44.000 UTC Sun Feb 11 2001
RTT Values:
NumOfRTT:10    RTTSum:32      RTTSum2:128
Packet Loss Values:
PacketLossSD:0 PacketLossDS:0
PacketOutOfSequence:0  PacketMIA:0    PacketLateArrival:0
InternalError:0        Busies:0
Jitter Values:
MinOfPositivesSD:4     MaxOfPositivesSD:4
NumOfPositivesSD:2     SumOfPositivesSD:8     Sum2PositivesSD:32
MinOfNegativesSD:4     MaxOfNegativesSD:4
NumOfNegativesSD:1     SumOfNegativesSD:4     Sum2NegativesSD:16
MinOfPositivesDS:0     MaxOfPositivesDS:0
NumOfPositivesDS:0     SumOfPositivesDS:0     Sum2PositivesDS:0
MinOfNegativesDS:4     MaxOfNegativesDS:4
NumOfNegativesDS:1     SumOfNegativesDS:4     Sum2NegativesDS:16
```

The values shown indicate the values for the last SAA operation. RTT stands for Round-Trip-Time. SD stands for Source-to-Destination. DS stands for Destination-to-Source. The * symbol in front of the time stamps indicate the time is synchronized using NTP or SNTP. For a description of the output fields, see the description in the **show rtr collection-statistics** command documentation.

Related Commands

Command	Description
show rtr configuration	Displays configuration values including all defaults for all SAA operations or the specified operation.

show rtr reaction-trigger

To display the reaction trigger information for all Service Assurance Agent (SAA) operations or the specified operation, use the **show rtr reaction-trigger** command in EXEC mode.

show rtr reaction-trigger [*operation-number*] [**tabular** | **full**]

Syntax Description

operation-number	(Optional) Number of the SAA operation to display.
tabular	(Optional) Display information in a column format reducing the number of screens required to display the information.
full	(Optional) Display all information using identifiers next to each displayed value. This is the default.

Defaults

Full format for all operations

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use the **show rtr reaction-trigger** command to display the configuration status and operational state of target operations that will be triggered as defined with the **rtr reaction-configuration** global command.

Examples

The following is sample output from the **show rtr reaction-trigger** command in full format:

```
Router# show rtr reaction-trigger 1

        Reaction Table
Entry Number: 1
Target Entry Number: 2
Status of Entry (SNMP RowStatus): active
Operational State: pending
```

Related Commands

Command	Description
show rtr configuration	Displays configuration values including all defaults for all SAA operations or the specified operation.

show rtr responder

To display Service Assurance Agent (SAA) Response Time Report (RTR) Responder information, use the **show rtr responder** command in EXEC mode.

show rtr responder

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

Use the **show rtr responder** command to display information about recent sources of SAA control messages, such as who has sent recent control messages and who has sent invalid control messages.

Examples

The following is sample output from the **show rtr responder** command:

```
Router# show rtr responder

RTR Responder is: Enabled
Number of control message received: 19 Number of errors: 1
Recent sources:
            4.0.0.1 [19:11:49.035 UTC Sat Dec 2 1995]
            4.0.0.1 [19:10:49.023 UTC Sat Dec 2 1995]
            4.0.0.1 [19:09:48.707 UTC Sat Dec 2 1995]
            4.0.0.1 [19:08:48.687 UTC Sat Dec 2 1995]
            4.0.0.1 [19:07:48.671 UTC Sat Dec 2 1995]

Recent error sources:
            4.0.0.1 [19:10:49.023 UTC Sat Dec 2 1995] RTT_AUTH_FAIL
```

Related Commands

Command	Description
show rtr configuration	Displays configuration values for SAA operations.

show rtr totals-statistics

To display the total statistical values (accumulation of error counts and completions) for all Service Assurance Agent (SAA) operations or the specified operation, use the **show rtr totals-statistics** command in EXEC mode.

show rtr totals-statistics [*number*] [**tabular** | **full**]

Syntax Description

number	(Optional) Number of the SAA operation to display.
tabular	(Optional) Display information in a column format reducing the number of screens required to display the information.
full	(Optional) Display all information using identifiers next to each displayed value. This is the default.

Defaults

Full format for all operations

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The total statistics consist of the following items:

- The operation number
- The start time of the current hour of statistics
- The age of the current hour of statistics
- The number of attempted operations

You can also use the **show rtr distributions-statistics** and **show rtr collection-statistics** commands to display additional statistical information.

Examples

The following is sample output from the **show rtr totals-statistics** command in full format:

```
Router# show rtr totals-statistics

        Statistic Totals
Entry Number: 1
Start Time Index: *17:15:41.000 UTC Thu May 16 1996
Age of Statistics Entry (hundredths of seconds): 48252
Number of Initiations: 10
```

Related Commands

Command	Description
show rtr collection-statistics	Displays statistical errors for all SAA operations or the specified operation.
show rtr configuration	Displays configuration values including all defaults for all SAA operations or the specified operation.
show rtr distributions-statistics	Displays statistic distribution information (captured response times) for all SAA operations or the specified operation.

show running-config

To display the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or virtual circuit (VC) class, use the **show running-config** command in privileged EXEC mode.

show running-config [*options*]

Syntax Description

options	(Optional) One of the following options can be entered with the command: • **brief**—Displays the configuration without certification data. • **class-map** *name*—Displays class map information. The **linenum** keyword can be used with the **class-map** *name* option. • **full**—Displays the full configuration. • **interface** *type number*—Displays interface-specific configuration information. If you use the **interface** keyword, you must specify the interface type and the interface number (for example, **interface ethernet 0**). Common interfaces include **async**, **ethernet**, **fastEthernet**, **group-async**, **loopback**, **null**, **serial**, and **virtual-template**. Use the **show run interface ?** command to determine the interfaces available on your system. • **linenum**—Displays line numbers in the output. The **brief** or **full** keyword can be used with the **linenum** keyword. • **map-class**—Displays map class information. This option is described separately; see the **show running-config map-class** command page. • **policy-map** *name*—Displays policy map information. The **linenum** keyword can be used with the **policy-map** *name* option. • **vc-class** *name*—Displays VC class information (display available only on limited routers such as the Cisco 7500 series). The **linenum** keyword can be used with the **vc-class** *name* option. • |—Allows addition of output modifiers and is available with all the keywords for this command.

Defaults

The **show running-config** command without any arguments or keywords displays the entire contents of the running configuration file.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.0	This command was replaced by the **more system:running-config** command.

12.0(1)T	The output modifier (|) was added.
12.2(4)T	The **linenum** keyword was added.

Usage Guidelines

The **show running-config** command is technically a command alias of the **more system:running-config** command. Although **more** commands are recommended (due to their uniform structure across platforms and their expandable syntax), the **show running-config** command remains enabled to accommodate its widespread use, and to allow typing shortcuts such as **show run**.

The **show running-config interface** command is useful when there are multiple interfaces and you want to look at the configuration of a specific interface.

The **linenum** keyword causes line numbers to be displayed in the output. This option is useful for identifying a particular portion of a very large configuration.

Examples

The following example shows the configuration for serial interface 1:

```
Router# show running-config interface serial 1

Building configuration...

Current configuration:
!
interface Serial1
 no ip address
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 shutdown
end
```

The following example shows the configuration for Ethernet interface 0/0. Line numbers are displayed in the output.

```
Router# show running-config interface ethernet 0/0 linenum

Building configuration...

Current configuration : 104 bytes
 1 : !
 2 : interface Ethernet0/0
 3 :  ip address 10.4.2.63 255.255.255.0
 4 :  no ip route-cache
 5 :  no ip mroute-cache
 6 : end
```

The following example shows how to set line numbers in the command output, and then use the output modifier to start the display at line 10:

```
Router# show running-config linenum | begin 10

   10 : boot-start-marker
   11 : boot-end-marker
   12 : !
   13 : no logging buffered
   14 : enable password #####
   15 : !
   16 : spe 1/0 1/7
   17 :  firmware location bootflash:mica-modem-pw.2.7.1.0.bin
```

```
18 : !
19 : !
20 : resource-pool disable
21 : !
22 : no aaa new-model
23 : ip subnet-zero
24 : ip domain name cisco.com
25 : ip name-server 172.16.11.48
26 : ip name-server 172.16.2.133
27 : !
28 : !
29 : isdn switch-type primary-5ess
30 : !
.
.
.
126 : end
```

Related Commandsd

Command	Description
boot config	Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).
configure terminal	Enters global configuration mode.
copy running-config startup-config	Copies the running configuration to the startup configuration. (Command alias for the **copy system:running-config nvram:startup-config** command.)
show startup-config	Displays the contents of NVRAM (if present and valid) or displays the configuration file pointed to by the CONFIG_FILE environment variable. (Command alias for the **more:nvram startup-config** command.)

show running-config map-class

To display only map-class configuration information from the running configuration file, use the **show running-config map-class** command in privileged EXEC mode.

show running-config map-class [**atm** [*map-class-name*] | **dialer** [*map-class-name*] | **frame-relay** [*map-class-name*]] [**linenum**]

Syntax Description

atm	(Optional) Displays only ATM map-class configuration lines.
dialer	(Optional) Displays only dialer map-class configuration lines.
frame-relay	(Optional) Displays only Frame Relay map-class configuration lines.
map-class-name	(Optional) Displays only configuration lines for the specified map-class.
linenum	(Optional) Displays line numbers in the output.

Defaults

Displays all map-class configuration in the running configuration file.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1	The **map-class** extension to the **show running-config** command was introduced to show only lines pertaining to dialer or Frame Relay map classes.
12.1(2)T	The **atm**, **dialer**, and **frame-relay** keywords and *map-class-name* argument were introduced.
12.2(4)T	The **linenum** keyword was added.

Usage Guidelines

Use the **show running-config map-class** command to display the following information from the running configuration file:

- All map classes configured on the router.
- Map classes configured specifically for ATM, Frame Relay, or dialer.
- A specific ATM, Frame Relay, or dialer map class.

Use the **linenum** keyword to display line numbers in the output. This option is useful for identifying a particular portion of a very large configuration.

Examples

All Map Classes Configured on the Router Example

The following example displays all map classes configured on the router:

```
Router# show running-config map-class

Building configuration...
Current configuration:
```

```
!
map-class frame-relay cir60
 frame-relay bc 16000
 frame-relay adaptive-shaping becn
!
map-class frame-relay cir70
 no frame-relay adaptive-shaping
 frame-relay priority-group 2
!
map-class atm vc100
 atm aal5mux
!
map-class dialer dialer1
 dialer idle-timeout 10
end
```

All Frame Relay Map Classes Example

The following example displays all Frame Relay map classes on the router:

```
Router# show running-config map-class frame-relay

Building configuration...
Current configuration:
!
map-class frame-relay cir60
 frame-relay bc 16000
 frame-relay adaptive-shaping becn
!
map-class frame-relay cir70
 no frame-relay adaptive-shaping
 frame-relay priority-group 2
end
```

A Specific Map Class and Display of Line Numbers Example

The following example displays a specific map class called class1. Line numbers are displayed in the output.

```
Router# show running-config map-class frame-relay class1 linenum

Building configuration...

Current configuration:
1 : !
2 : map-class frame-relay boy
3 :  no frame-relay adaptive-shaping
4 :  frame-relay cir 1000
5 : end
```

Related Commands

Command	Description
map-class atm	Specifies the ATM map class for an SVC.
map-class dialer	Defines a class of shared configuration parameters associated with the dialer map command for outgoing calls from an ISDN interface and for PPP callback.
map-class frame-relay	Specifies a map class to define QoS values for a Frame Relay VC.
more system:running-config	Displays contents of the currently running configuration file (equivalent to the **show running-config** command.)

show saa apm cache

To display the amount of memory available in the Service Assurance Agent (SAA) Application Performance Monitor (APM) cache and information about the files stored in the cache, use the **show saa apm cache** command in EXEC mode.

show saa apm cache

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

SAA APM script and scheduler files are kept in an area of system memory called the SAA APM cache.

Examples

The following is sample output from the **show saa apm cache** command:

```
Router# show saa apm cache

 Cache Size (bytes): 100000
 Cache used (bytes): 6849

TimeCreated    TimeAccessed    Size  Ref Loc Type SBit FileName
03/21 13:31:25 03/21 13:31:48   1170   0   1  SCR    0 user/scripts/ldap-rem.scr
03/21 13:31:23 03/21 13:31:48     38   0   1  DAT    0 user/data/ldap-rem.dat
03/21 13:31:22 03/21 13:31:27     69   1   0  DAT    0 user/data/ldap.dat
03/21 13:31:20 03/21 13:31:27   1513   1   0  SCR    0 user/scripts/ldap.scr
03/21 13:31:19 03/21 13:31:27   2500   1   0  SCH    0 user/scheduler/master.sch
03/21 13:31:17 03/21 13:31:27    256   1   0  CFG    0 apm.cfg.1
03/21 13:31:17 03/21 13:31:17    568   1   0  CFG    0 user/config/ldap.cf
03/20 14:29:13 03/20 14:29:36    735   0   1  SCR    0 user/scripts/udp-rem.scr
```

Table 105 describes the significant fields shown in the display.

Table 105 show saa apm cache Field Descriptions

Field	Description
Type	Type of file in the cache. Possible types are: • CFG— APM configuration file • DAT — APM data file • SCR—APM script file • SCH—APM scheduler file
Size	Size of the file, in bytes.

Table 105 show saa apm cache Field Descriptions

Field	Description
Ref	Ref-count. Indicates how many APM operations are accessing (referencing) the file.
Loc	"Local" value. Indicates whether the file is local or remote. Possible values are: 0—File is remote. 1—File is local.
SBit	"Sticky bit" value. Possible values are: 0—sticky bit not set; this file will be deleted from the APM cache during the next cache trimming operation, or when a **clear saa apm cache** command is executed. 1—sticky bit is set; this file can only be deleted by using the **force** keyword with the **clear saa apm cache** command.

Related Commands

Command	Description
clear saa apm cache	Deletes files from the SAA Application Performance Monitor cache.
saa apm cache-size	Sets the size of the SAA Application Performance Monitor (APM) cache.
show saa apm operation	Displays details about SAA Application Performance Monitor (APM).

show saa apm information

To display details about Service Assurance Agent (SAA) Application Performance Monitor (APM) running on the system, use the **show saa apm information** command in EXEC mode.

show saa apm information

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.

Examples

The following is sample output from the **show saa apm information** command:

```
Router# show saa apm information

      Service Assurance Agent: Application Performance Monitor

      APM Engine Version: 1.0
Max Number of oper supported: 50
 Number of configurable oper: 50
   Number of oper configured: 0
    Number of files in cache: 0
          Cache Size (bytes): 100000
          Cache used (bytes): 0
  APM low memory water-mark: 6708828
```

Related Commands

Command	Description
saa apm lowWaterMark	Specifies the lowest amount of free memory that must be available on the system to allow additional SAA APM operations to be configured.

show saa apm operation

To display details about Service Assurance Agent (SAA) Application Performance Monitor (APM) operation, use the **show saa apm operation** command in EXEC mode.

show saa apm operation [*operation-number*]

Syntax Description

operation-number	(Optional) Number that uniquely identifies an APM operation.

Defaults

Information for all APM operations is displayed.

Command Modes

EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.

Examples

The following is sample output from the **show saa apm operation** command:

```
Router# show saa apm operation

         Operation Information:

 Operation ID: 1234567
 Owner: CLI
 ControlFile URL: ftp://user:password@saa-nms/apm/config/smtp-1000.cfg
 SNMP Row Status: active
 Latest Operation Time: *08:13:40.000 UTC Mon Oct 08 2001
 Latest Operation Status: 0
```

show saa apm results

To display the accumulated data for Service Assurance Agent (SAA) Application Performance Monitor (APM) operations, use the **show saa apm results** command in EXEC mode.

show saa apm results [*operation-number*]

Syntax Description

operation-number	(Optional) A number that uniquely identifies an APM operation. If an *operation-number* is not specified, all operation results in the buffer are displayed.

Defaults

All APM operation results are displayed.

Command Modes

EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

SAA APM script and scheduler files are kept in an area of system memory called the SAA APM cache.

Examples

The following is sample output from the **show saa apm results** command:

```
Router# show saa apm results

 Cache Size (bytes): 100000
 Cache used (bytes): 14188

 File Name                                TimeCreated TimeAccessed ref Type sticky
 apm/data/ldap-13.dat                        13:37:20     13:37:25   1 DAT  0
 apm.cf.9                                    13:37:18     13:37:25   1 CFG  0
 apm/config/ldap-13.cf                       13:37:18     00:00:00   1 CFG  0
 apm/data/ldap-12.dat                        13:37:15     13:37:20   1 DAT  0
 apm.cf.8                                    13:37:14     13:37:20   1 CFG  0
 apm/config/ldap-12.cf                       13:37:14     00:00:00   1 CFG  0
 apm/data/ldap-11.dat                        13:37:11     13:37:16   1 DAT  0
 apm.cf.7                                    13:37:11     13:37:16   1 CFG  0
 apm/config/ldap-11.cf                       13:37:11     00:00:00   1 CFG  0
 apm/scripts/ldap.scr                        13:37:07     13:37:29   3 SCR  0
 apm/data/iptv-2.dat                         13:36:49     13:36:54   1 DAT  0
 apm/config/iptv-2.cf                        13:36:48     00:00:00   1 CFG  0
 apm/scripts/iptv.scr                        13:36:47     13:37:08   1 SCR  0
 apm/scheduler/master.sch                    13:36:45     13:37:34   4 SCH  0
```

Table 106 describes the significant fields shown in the display.

Table 106 show saa apm cache Field Descriptions

Field	Description
Type	Type of file in cache. Possible types are: • CFG— APM configuration file • DAT — APM data file • SCR—APM script file • SCH—APM scheduler file
sticky	"Sticky bit" value. Possible values are: 0—sticky bit not set; this file will be deleted from the APM cache during the next cache trimming operation, or when a **clear saa apm cache** command is executed. 1—sticky bit is set; this file can only be deleted by using the **force** keyword with the **clear saa apm cache** command.

Related Commands

Command	Description
clear saa apm cache	Deletes files from the SAA Application Performance Monitor cache.
saa apm cache-size	Sets the size of the SAA Application Performance Monitor cache.
show saa apm operation	Displays details about SAA Application Performance Monitor operations.

show snmp

To check the status of Simple Network Management Protocol (SNMP) communications, use the **show snmp** command in EXEC mode.

show snmp

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command provides counter information for SNMP operations. It also displays the chassis ID string defined with the **snmp-server chassis-id** global configuration command.

Examples

The following is sample output from the **show snmp** command:

```
Router# show snmp

Chassis: 01506199
37 SNMP packets input
    0 Bad SNMP version errors
    4 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    24 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    28 Get-next PDUs
    0 Set-request PDUs
78 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    24 Response PDUs
    13 Trap PDUs

SNMP logging: enabled
    Logging to 172.16.58.33.162, 0/10, 13 sent, 0 dropped.


SNMP Manager-role output packets
    4 Get-request PDUs
    4 Get-next PDUs
    6 Get-bulk PDUs
    4 Set-request PDUs
    23 Inform-request PDUs
    30 Timeouts
```

```
    0 Drops
SNMP Manager-role input packets
    0 Inform response PDUs
    2 Trap PDUs
    7 Response PDUs
    1 Responses with errors

SNMP informs: enabled
    Informs in flight 0/25 (current/max)
    Logging to 172.16.217.141.162
        4 sent, 0 in-flight, 1 retries, 0 failed, 0 dropped
    Logging to 172.16.58.33.162
        0 sent, 0 in-flight, 0 retries, 0 failed, 0 dropped
```

Table 107 describes the significant fields shown in the display.

Table 107 show snmp Field Descriptions

Field	Description
Chassis	Chassis ID string.
SNMP packets input	Total number of SNMP packets input.
Bad SNMP version errors	Number of packets with an invalid SNMP version.
Unknown community name	Number of SNMP packets with an unknown community name.
Illegal operation for community name supplied	Number of packets requesting an operation not allowed for that community.
Encoding errors	Number of SNMP packets that were improperly encoded.
Number of requested variables	Number of variables requested by SNMP managers.
Number of altered variables	Number of variables altered by SNMP managers.
Get-request PDUs	Number of get requests received.
Get-next PDUs	Number of get-next requests received.
Set-request PDUs	Number of set requests received.
SNMP packets output	Total number of SNMP packets sent by the router.
Too big errors	Number of SNMP packets which were larger than the maximum packet size.
Maximum packet size	Maximum size of SNMP packets.
No such name errors	Number of SNMP requests that specified a MIB object that does not exist.
Bad values errors	Number of SNMP set requests that specified an invalid value for a MIB object.
General errors	Number of SNMP set requests that failed due to some other error. (It was not a noSuchName error, badValue error, or any of the other specific errors.)
Response PDUs	Number of responses sent in reply to requests.
Trap PDUs	Number of SNMP traps sent.
SNMP logging	Indicates whether logging is enabled or disabled.
sent	Number of traps sent.

Table 107 show snmp Field Descriptions (continued)

Field	Description
dropped	Number of traps dropped. Traps are dropped when the trap queue for a destination exceeds the maximum length of the queue, as set by the **snmp-server queue-length** global configuration command.
SNMP Manager-role output packets	Information related to packets sent by the router as an SNMP manager.
Get-request PDUs	Number of get requests sent.
Get-next PDUs	Number of get-next requests sent.
Get-bulk PDUs	Number of get-bulk requests sent.
Set-request PDUs	Number of set requests sent.
Inform-request PDUs	Number of inform requests sent.
Timeouts	Number of request timeouts.
Drops	Number of requests dropped. Reasons for drops include no memory, a bad destination address, or an unreasonable destination address.
SNMP Manager-role input packets	Information related to packets received by the router as an SNMP manager.
Inform response PDUs	Number of inform request responses received.
Trap PDUs	Number of SNMP traps received.
Response PDUs	Number of responses received.
Responses with errors	Number of responses containing errors.
SNMP informs	Indicates whether SNMP informs are enabled.
Informs in flight	Current and maximum possible number of informs waiting to be acknowledged.
Logging to	Destination of the following informs.
sent	Number of informs sent to this host.
in-flight	Number of informs currently waiting to be acknowledged.
retries	Number of inform retries sent.
failed	Number of informs that were never acknowledged.
dropped	Number of unacknowledged informs that were discarded to make room for new informs.

Related Commands

Command	Description
show snmp pending	Displays the current set of pending SNMP requests.
show snmp sessions	Displays the current SNMP sessions.
snmp-server chassis-id	Provides a message line identifying the SNMP server serial number.
snmp-server manager	Starts the SNMP manager process.
snmp-server manager session-timeout	Sets the amount of time before a nonactive session is destroyed.
snmp-server queue-length	Establishes the message queue length for each trap host.

show snmp engineID

To display the identification of the local Simple Network Management Protocol (SNMP) engine and all remote engines that have been configured on the router, use the **show snmp engineID** command in EXEC mode.

show snmp engineID

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

An SNMP engine is a copy of SNMP that can reside on a local or remote device.

Examples

The following example specifies 00000090200000000C025808 as the local engineID and 123456789ABCDEF000000000 as the remote engine ID, 172.16.37.61 as the IP address of the remote engine (copy of SNMP) and 162 as the port from which the remote device is connected to the local device:

```
Router# show snmp engineID

Local SNMP engineID: 00000090200000000C025808
Remote Engine ID          IP-addr          Port
123456789ABCDEF000000000  172.16.37.61     162
```

Table 108 describes the fields shown in the display.

Table 108 show snmp engineID Field Descriptions

Field	Definition
Local SNMP engine ID	A string that identifies the copy of SNMP on the local device.
Remote Engine ID	A string that identifies the copy of SNMP on the remote device.
IP-addr	The IP address of the remote device.
Port	The port number on the local device to which the remote device is connected.

Related Commands

Command	Description
snmp-server engineID local	Configures a name for either the local or remote SNMP engine on the router.

show snmp group

To display the names of groups on the router and the security model, the status of the different views, and the storage type of each group, use the **show snmp group** command in EXEC mode.

show snmp group

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.

Examples

The following example specifies the group name as public, the security model as v1, the read view name as v1default, the notify view name as *tv.FFFFFFFF, and the storage type as volatile:

```
router# show snmp group

groupname: public      security model:v1
readview:v1default
writeview:  no writeview specified
notifyview: *tv.FFFFFFFF
storage-type: volatile
```

Table 109 describes the fields shown in the example.

Table 109 show snmp group Field Descriptions

Field	Definition
groupname	The name of the SNMP group, or collection of users that have a common access policy.
security model	The security model used by the group, either v1, v2c, or v3.
readview	A string identifying the read view of the group.
writeview	A string identifying the write view of the group.
notifyview	A string identifying the notify view of the group.
storage-type	Indicates whether the settings have been set in volatile or temporary memory on the device, or in nonvolatile or persistent memory where settings will remain after the device has been turned off and on again.

Related Commands

Command	Description
snmp-server group	Configures a new SNMP group or a table that maps SNMP users to SNMP views.

show snmp mib

To display a list of the MIB module instance identifiers (OIDs) registered on your system, use the **show snmp mib** command in EXEC mode.

show snmp mib

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.2, 12.2(2)T	This command was introduced.

Usage Guidelines

SNMP management information is viewed as a collection of managed objects, residing in a virtual information store, termed the Management Information Base (MIB). Collections of related objects are defined in MIB modules. These modules are written using a subset of OSIs Abstract Syntax Notation One (ASN.1), termed the Structure of Management Information (SMI).

This command is intended for network administrators who are familiar with the SMI and ASN.1 syntax.

While this command can be used to display a list of MIB object identifiers (OIDs) registered on the system, the use of a network management system (NMS) application is the recommended alternative for gathering this information.

The **show snmp mib** command will display the instance identifiers for all the MIB objects on the system. The instance identifier is the final part of the OID. An object can have one or more instance identifiers. Before displaying the instance identifier, the system attempts to find the best match with the list of table names. The MIB module table names are registered when the system initializes.

The definitions for the OIDs displayed by this command can be found in the relevant RFCs and MIB modules. For example, RFC 1907 defines the system.x, sysOREntry.x, snmp.x, and snmpTrap.x OIDs, and this information is supplemented by the extensions defined in the CISCO-SYSTEM-MIB.

Tips This command produces a high volume of output if SNMP is enabled on your system. To exit from a --More-- prompt, press Ctrl-Z.

Examples

The following is sample output from the **show snmp mib** command:

```
Router# show snmp mib

system.1
system.2
sysUpTime
system.4
system.5
system.6
system.7
```

```
system.8
sysOREntry.2
sysOREntry.3
sysOREntry.4
interfaces.1
ifEntry.1
ifEntry.2
ifEntry.3
ifEntry.4
ifEntry.5
ifEntry.6
ifEntry.7
ifEntry.8
ifEntry.9
ifEntry.10
ifEntry.11
 --More--
 .
 .
 .
captureBufferEntry.2
captureBufferEntry.3
captureBufferEntry.4
captureBufferEntry.5
captureBufferEntry.6
captureBufferEntry.7
capture.3.1.1
eventEntry.1
eventEntry.2
eventEntry.3
eventEntry.4
eventEntry.5
eventEntry.6
eventEntry.7
logEntry.1
logEntry.2
logEntry.3
logEntry.4
rmon.18.1.1.2
rmon.18.1.1.3
rmon.18.1.1.4
rmon.18.1.1.5
rmon.18.1.1.6
rmon.18.1.1.7
rmon.18.2.1.2
rmon.18.2.1.3
rmon.18.3.1.2
--More--
 .
 .
 .
rmon.19.11.1.1
rmon.19.11.1.2
rmon.19.11.1.3
rmon.19.12
rmon.19.13.1.2
rmon.19.13.1.3
rmon.19.13.1.4
rmon.19.13.1.5
rmon.19.13.1.6
rmon.19.14.1.2
rmon.19.14.1.3
rmon.19.14.1.4
rmon.19.14.1.5
```

```
rmon.19.14.1.6
rmon.19.14.1.7
rmon.19.14.1.8
rmon.19.14.1.9
rmon.19.15
rmon.19.16
dot1dBase.1
dot1dBase.2
dot1dBase.3
dot1dBasePortEntry.1
dot1dBasePortEntry.2
dot1dBasePortEntry.3
dot1dBasePortEntry.4
--More--
 .
 .
 .
ifXEntry.1
ifXEntry.2
ifXEntry.3
ifXEntry.4
ifXEntry.5
ifXEntry.6
ifXEntry.7
ifXEntry.8
ifXEntry.9
ifXEntry.10
ifXEntry.11
ifXEntry.12
ifXEntry.13
ifXEntry.14
ifXEntry.15
ifXEntry.16
ifXEntry.17
ifXEntry.18
ifXEntry.19
ifStackEntry.3
ifTestEntry.1
ifTestEntry.2
--More--
 .
 .
 .
```

Related Commands

Command	Description
show snmp mib ifmib ifindex	Displays SNMP Interface Index identification numbers (ifIndex values) for all the system interfaces or the specified system interface

show snmp mib ifmib ifindex

To display SNMP Interface Index identification numbers (ifIndex values) for all the system interfaces or the specified system interface, use the **show snmp mib ifmib ifindex** command in EXEC mode.

show snmp mib ifmib ifindex [*interface-type*] [*slot/*][*port-adapter/*][*port*]

Syntax Description

interface-type	The type of interface. Use the **show snmp mib ifmib ifindex ?** command to determine the options available on your system. Typical interface-types include **async**, **dialer**, **ethernet**, **fastEthernet**, **serial** and so on.
slot/	The slot number for the interface card, followed by a forward-slash. The availability of this argument depends on your system hardware configuration.
port-adapter/	The port-adapter number, followed by a forward-slash. The availability of this argument depends on your system hardware configuration.
port	The interface number.

Defaults

The ifIndex values for all interfaces are displayed.

Command Modes

EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

The **show snmp mib ifmib ifindex** command allows you to display SNMP Interface Index identification numbers (ifIndex values) assigned to interfaces and subinterfaces using the CLI. This command provides a way to view these values without the need for a Network Management Station.

If a specific interface is not specified using the optional *interface-type*, *slot*, *port-adapter*, and *port* arguments, the ifDescr and ifIndex pairs of all interfaces and subinterfaces present on the system are shown.

Examples

The following example shows output for a specific interface:

```
Router# show snmp mib ifmib ifIndex Ethernet2/0
Ethernet2/0: Ifindex = 2
```

The following examples shows output for all interfaces:

```
Router# show snmp mib ifmib ifindex

ATM1/0: Ifindex = 1
ATM1/0-aal5 layer: Ifindex = 12
ATM1/0-atm layer: Ifindex = 10
ATM1/0.0-aal5 layer: Ifindex = 13
```

```
ATM1/0.0-atm subif: Ifindex = 11
ATM1/0.9-aal5 layer: Ifindex = 32
ATM1/0.9-atm subif: Ifindex = 31
ATM1/0.99-aal5 layer: Ifindex = 36
ATM1/0.99-atm subif: Ifindex = 35
Ethernet2/0: Ifindex = 2
Ethernet2/1: Ifindex = 3
Ethernet2/2: Ifindex = 4
Ethernet2/3: Ifindex = 5
Null0: Ifindex = 14
Serial3/0: Ifindex = 6
Serial3/1: Ifindex = 7
Serial3/2: Ifindex = 8
Serial3/3: Ifindex = 9
```

Related Commands

Command	Description
show snmp mib	Displays a list of the MIB module instance identifiers (OIDs) registered on the system.
snmp ifindex persist	Enables ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots only on a specific interface.
snmp ifmib ifalias long	Configures the system to handle IfAlias descriptions of up to 256 characters in length.
snmp-server ifindex persist	Enables ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots for all interfaces (globally).

show snmp mib notification-log

To display information about the state of local SNMP notification logging, use the **show snmp mib notification-log** command in EXEC mode.

show snmp mib notification-log [**all** | **default**]

Syntax Description

all	(Optional) Displays all notification log entries stored in the local Notification Log MIB database.
default	(Optional) Displays summary information for the default (unnamed) SNMP Notification Log.

Command Modes

EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Release 12.2(13)T.

Usage Guidelines

The SNMP Notification Log works in conjunction with the NOTIFICATION-LOG-MIB.my MIB module (available at ftp://ftp.cisco.com/pub/mibs/v2/). This MIB module is based on RFC 3014. The local logs can be polled by external network management applications to verify that they have not missed important SNMP notifications (traps and informs).

The **show snmp mib notification-log all** command displays all logged notification entries currently in the local MIB database. Entries are displayed from the oldest to the newest. The time of entry creation is determined using the system-up-time (sysUpTime) value; this means that the age of the entry is set using the amount of time that has passed since the router was last restarted. Other information for the entries includes the notificationID, and the filters (varbinds) associated with the log, if any.

Examples

The following is sample output from the **show snmp mib notification-log** command:

```
Router# show snmp mib notification-log

GlobalAgeout 15, GlobalEntryLimit 500
Total Notifications logged in all logs 0
Log Name"", Log entry Limit 500, Notifications logged 0
Logging status enabled
Created by cli
```

Note that in this example, the Log Name of "" indicates the default "null-named" Notification Log.

Related Commands

Command	Description
snmp mib notification-log default	Creates and activates an SNMP Notification Log.

Command	Description
snmp mib notification-log globalageout	Sets the maximum age for a notification.
snmp mib notification-log globalsize	Sets the maximum number of notifications allowed in all logs.

show snmp pending

To display the current set of pending Simple Network Management Protocol (SNMP) requests, use the **show snmp pending** command in EXEC mode.

show snmp pending

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

After the SNMP manager sends a request, the request is "pending" until the manager receives a response or the request timeout expires.

Examples

The following is sample output from the **show snmp pending** command:

```
Router# show snmp pending

req id: 47, dest: 172.16.58.33.161, V2C community: public, Expires in 5 secs
req id: 49, dest: 172.16.58.33.161, V2C community: public, Expires in 6 secs
req id: 51, dest: 172.16.58.33.161, V2C community: public, Expires in 6 secs
req id: 53, dest: 172.16.58.33.161, V2C community: public, Expires in 8 secs
```

Table 110 describes the significant fields shown in the display.

Table 110 show snmp pending Field Descriptions

Field	Description
req id	ID number of the pending request.
dest	IP address of the intended receiver of the request.
V2C community	SNMP version 2C community string sent with the request.
Expires in	Remaining time before request timeout expires.

Related Commands

Command	Description
show snmp	Checks the status of SNMP communications.
show snmp sessions	Displays the current SNMP sessions.
snmp-server manager	Starts the SNMP manager process.
snmp-server manager session-timeout	Sets the amount of time before a nonactive session is destroyed.

show snmp sessions

To display the current Simple Network Management Protocol (SNMP) sessions, use the **show snmp sessions** command in EXEC mode.

show snmp sessions [**brief**]

Syntax Description

brief	(Optional) Displays a list of sessions only. Does not display session statistics.

Command Modes

EXEC

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Sessions are created when the SNMP manager in the router sends SNMP requests, such as inform requests, to a host or receives SNMP notifications from a host. One session is created for each destination host. If there is no further communication between the router and host within the session timeout period, the corresponding session will be deleted.

Examples

The following is sample output from the **show snmp sessions** command:

```
Router# show snmp sessions

Destination: 172.16.58.33.162, V2C community: public
  Round-trip-times: 0/0/0 (min/max/last)
  packets output
    0 Gets, 0 GetNexts, 0 GetBulks, 0 Sets, 4 Informs
    0 Timeouts, 0 Drops
  packets input
    0 Traps, 0 Informs, 0 Responses (0 errors)
Destination: 172.16.217.141.162, V2C community: public, Expires in 575 secs
  Round-trip-times: 1/1/1 (min/max/last)
  packets output
    0 Gets, 0 GetNexts, 0 GetBulks, 0 Sets, 4 Informs
    0 Timeouts, 0 Drops
  packets input
    0 Traps, 0 Informs, 4 Responses (0 errors)
```

Table 111 describes the significant fields shown in the output.

The following is sample output from the **show snmp sessions brief** command:

```
Router# show snmp sessions brief

Destination: 172.16.58.33.161, V2C community: public, Expires in 55 secs
```

Table 111 describes the significant fields shown in the display.

Table 111 show snmp sessions Field Descriptions

Field	Description
Destination	IP address of the remote agent.
V2C community	SNMP version 2C community string used to communicate with the remote agent.
Expires in	Remaining time before the session timeout expires.
Round-trip-times	Minimum, maximum, and the last round-trip time to the agent.
packets output	Packets sent by the router.
Gets	Number of get requests sent.
GetNexts	Number of get-next requests sent.
GetBulks	Number of get-bulk requests sent.
Sets	Number of set requests sent.
Informs	Number of inform requests sent.
Timeouts	Number of request timeouts.
Drops	Number of packets that could not be sent.
packets input	Packets received by the router.
Traps	Number of traps received.
Informs	Number of inform responses received.
Responses	Number of request responses received.
errors	Number of responses that contained an SNMP error code.

Related Commands

Command	Description
show snmp	Checks the status of SNMP communications.
show snmp pending	Displays the current set of pending SNMP requests.
snmp-server manager	Starts the SNMP manager process.
snmp-server manager session-timeout	Sets the amount of time before a nonactive session is destroyed.

show snmp user

To display information on each Simple Network Management Protocol (SNMP) username in the group username table, use the **show snmp user** command in EXEC mode.

show snmp user

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

An SNMP user is a remote user for which an SNMP management operation is performed. For example, inform operations can be sent to a user on a remote SNMP engine. The user is designated using the **snmp-server user** command.

Examples

The following example specifies the username as authuser, the engine ID string as 00000090200000000C025808, and the storage-type as nonvolatile:

```
Router# show snmp user

User name: authuser
Engine ID: 00000090200000000C025808
storage-type: nonvolatile
```

Table 112 describes the fields shown in the display.

Table 112 show snmp user Field Descriptions

Field	Definition
User name	A string identifying the name of the SNMP user.
Engine ID	A string identifying the name of the copy of SNMP on the device.
storage-type	Indicates whether the settings have been set in volatile or temporary memory on the device, or in nonvolatile or persistent memory where settings will remain after the device has been turned off and on again.

Related Commands

Command	Description
snmp-server user	Configures a new user to an SNMP group.

show sntp

To show information about the Simple Network Time Protocol (SNTP), use the **show sntp** command in EXEC mode on a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router.

show sntp

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Examples

The following is sample output from the **show sntp** command:

```
Router> show sntp

SNTP server     Stratum   Version    Last Receive
172.16.118.9       5         3        00:01:02
172.21.28.34       4         3        00:00:36    Synced  Bcast

Broadcast client mode is enabled.
```

Table 113 describes the significant fields shown in the display.

Table 113 show sntp Field Descriptions

Field	Description
SNTP server	Address of the configured or broadcast NTP server.
Stratum	NTP stratum of the server. The stratum indicates how far away from an authoritative time source the server is.
Version	NTP version of the server.
Last Receive	Time since the last NTP packet was received from the server.
Synced	Indicates the server chosen for synchronization.
Bcast	Indicates a broadcast server.

Related Commands

Command	Description
sntp broadcast client	Configures a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use SNTP to accept NTP traffic from any broadcast server.
sntp server	Configures a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use SNTP to request and accept NTP traffic from a time server.

show stacks

To monitor the stack usage of processes and interrupt routines, use the **show stacks** command in EXEC mode.

show stacks

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The display from this command includes the reason for the last system reboot. If the system was reloaded because of a system failure, a saved system stack trace is displayed. This information is of use only to your technical support representative in analyzing crashes in the field. It is included here in case you need to read the displayed statistics to an engineer over the phone.

Examples

The following is sample output from the **show stacks** command following a system failure:

```
Router# show stacks

Minimum process stacks:
Free/Size  Name
 652/1000  Router Init
 726/1000  Init
 744/1000  BGP Open
 686/1200  Virtual Exec

Interrupt level stacks:
Level    Called Free/Size  Name
  1           0 1000/1000  env-flash
  3         738  900/1000  Multiport Communications Interfaces
  5         178  970/1000  Console UART
System was restarted by bus error at PC 0xAD1F4, address 0xD0D0D1A
GS Software (GS3), Version 9.1(0.16), BETA TEST SOFTWARE
Compiled Tue 11-Aug-92 13:27 by jthomas
Stack trace from system failure:
FP: 0x29C158, RA: 0xACFD4
FP: 0x29C184, RA: 0xAD20C
FP: 0x29C1B0, RA: 0xACFD4
FP: 0x29C1DC, RA: 0xAD304
FP: 0x29C1F8, RA: 0xAF774
FP: 0x29C214, RA: 0xAF83E
FP: 0x29C228, RA: 0x3E0CA
FP: 0x29C244, RA: 0x3BD3C
```

Related Commands

Command	Description
show processes	Displays information about the active processes.

show startup-config

The **more nvram:startup-config** command has been replaced by the **show startup-config** command. See the description of the **more** command in the "Cisco IOS File System Commands" chapter for more information.

show subsys

To display the subsystem information, use the **show subsys** command in privileged EXEC mode.

show subsys [**class** *class* | **name** *name*]

Syntax Description

class *class*	(Optional) Displays the subsystems of the specified class. Valid classes are **driver**, **kernel**, **library**, **management**, **protocol**, and **registry**.
name *name*	(Optional) Displays the specified subsystem. Use the asterisk character (*) as a wildcard at the end of the name to list all subsystems, starting with the specified characters.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Use the **show subsys** command to confirm that all required features are in the running image.

Examples

The following is sample output from the **show subsys** command:

```
Router# show subsys

                    Class         Version
static_map          Kernel      1.000.001
arp                 Kernel      1.000.001
ether               Kernel      1.000.001
compress            Kernel      1.000.001
alignment           Kernel      1.000.002
monvar              Kernel      1.000.001
slot                Kernel      1.000.001
oir                 Kernel      1.000.001
atm                 Kernel      1.000.001
ip_addrpool_sys     Library     1.000.001
chat                Library     1.000.001
dialer              Library     1.000.001
flash_services      Library     1.000.001
ip_localpool_sys    Library     1.000.001
nvram_common        Driver      1.000.001
ASP                 Driver      1.000.001
sonict              Driver      1.000.001
oc3suni             Driver      1.000.001
oc12suni            Driver      1.000.001
ds3suni             Driver      1.000.001
.
.
.
```

Table 114 describes the fields shown in the display.

Table 114 show subsys Field Descriptions

Field	Description
static_map	Name of the subsystem.
Class	Class of the subsystem. Possible classes include Kernel, Library, Driver, Protocol, Management, Registry, and SystemInit.
Version	Version of the subsystem.

show tcp

To display the status of TCP connections, use the **show tcp** command in EXEC mode.

show tcp [*line-number*]

Syntax Description

line-number	(Optional) Absolute line number of the line for which you want to display Telnet connection status.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample output from the **show tcp** command:

```
Router# show tcp

tty0, connection 1 to host cider
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 172.31.232.17, Local port: 11184
Foreign host: 172.31.1.137, Foreign port: 23

Enqueued packets for retransmit: 0, input: 0, saved: 0

Event Timers (current time is 67341276):
Timer:       Retrans   TimeWait    AckHold    SendWnd  KeepAlive
Starts:           30          0         32          0          0
Wakeups:           1          0         14          0          0
Next:              0          0          0          0          0

iss:   67317172  snduna:   67317228  sndnxt:   67317228     sndwnd:   4096
irs: 1064896000  rcvnxt: 1064897597  rcvwnd:       2144  delrcvwnd:      0

SRTT: 317 ms, RTTO: 900 ms, RTV: 133 ms, KRTT: 0 ms
minRTT: 4 ms, maxRTT: 300 ms, ACK hold: 300 ms
Flags: higher precedence, idle user, retransmission timeout

Datagrams (max data segment is 536 bytes):
Rcvd: 41 (out of order: 0), with data: 34, total data bytes: 1596
Sent: 57 (retransmit: 1), with data: 35, total data bytes: 55
```

Table 115 describes the first five lines of output shown in the display.

Table 115 show tcp Field Descriptions—First Section of Output

Field	Description
tty0	Identifying number of the line.
connection 1	Number identifying the TCP connection.
to host xxx	Name of the remote host to which the connection has been made.

Table 115 show tcp Field Descriptions—First Section of Output (continued)

Field	Description
Connection state is ESTAB	A connection progresses through a series of states during its lifetime. These states follow in the order in which a connection progresses through them. • LISTEN—Waiting for a connection request from any remote TCP and port. • SYNSENT—Waiting for a matching connection request after having sent a connection request. • SYNRCVD—Waiting for a confirming connection request acknowledgment after having both received and sent a connection request. • ESTAB—Indicates an open connection; data received can be delivered to the user. This is the normal state for the data transfer phase of the connection. • FINWAIT1—Waiting for a connection termination request from the remote TCP or an acknowledgment of the connection termination request previously sent. • FINWAIT2—Waiting for a connection termination request from the remote TCP host. • CLOSEWAIT—Waiting for a connection termination request from the local user. • CLOSING—Waiting for a connection termination request acknowledgment from the remote TCP host. • LASTACK—Waiting for an acknowledgment of the connection termination request previously sent to the remote TCP host. • TIMEWAIT—Waiting for enough time to pass to be sure the remote TCP host has received the acknowledgment of its connection termination request. • CLOSED—Indicates no connection state at all. For more information, see RFC 793, *Transmission Control Protocol Functional Specification.*
I/O status:	Number describing the current internal status of the connection.
unread input bytes:	Number of bytes that the lower-level TCP processes have read, but the higher-level TCP processes have not yet processed.
Local host:	IP address of the network server.
Local port:	Local port number, as derived from the following equation: *line-number* + (512 * *random-number*). (The line number uses the lower nine bits; the other bits are random.)
Foreign host:	IP address of the remote host to which the TCP connection has been made.
Foreign port:	Destination port for the remote host.

Table 115 show tcp Field Descriptions—First Section of Output (continued)

Field	Description
Enqueued packets for retransmit:	Number of packets waiting on the retransmit queue. These are packets on this TCP connection that have been sent but have not yet been acknowledged by the remote TCP host.
input:	Number of packets that are waiting on the input queue to be read by the user.
saved:	Number of received out-of-order packets that are waiting for all packets comprising the message to be received before they enter the input queue. For example, if packets 1, 2, 4, 5, and 6 have been received, packets 1 and 2 would enter the input queue, and packets 4, 5, and 6 would enter the saved queue.

The following line of output shows the current time according to the system clock of the local host:

```
Event Timers (current time is 67341276):
```

The time shown is the number of milliseconds since the system started.

The following lines of output display the number of times that various local TCP timeout values were reached during this connection. In this example, the local host re-sent data 30 times because it received no response from the remote host, and it sent an acknowledgment many more times because there was no data on which to piggyback.

```
Timer:        Retrans    TimeWait     AckHold     SendWnd  KeepAlive
Starts:            30           0          32           0          0
Wakeups:            1           0          14           0          0
Next:               0           0           0           0          0
```

Table 116 describes the fields in the preceding lines of output.

Table 116 show tcp Field Descriptions—Second Section of Output

Field	Description
Timer:	The names of the timers in the display.
Starts:	The number of times the timer has been started during this connection.
Wakeups:	Number of keepalives sent without receiving any response. (This field is reset to zero when a response is received.)
Next:	The system clock setting that will trigger the next time this timer will go off.
Retrans	The Retransmission timer is used to time TCP packets that have not been acknowledged and are waiting for retransmission.
TimeWait	The TimeWait timer is used to ensure that the remote system receives a request to disconnect a session.
AckHold	The Acknowledgment timer is used to delay the sending of acknowledgments to the remote TCP in an attempt to reduce network use.
SendWnd	The Send Window is used to ensure that there is no closed window due to a lost TCP acknowledgment.
KeepAlive	The KeepAlive timer is used to control the transmission of test messages to the remote TCP to ensure that the link has not been broken without the local TCP's knowledge.

The following lines of output display the sequence numbers that TCP uses to ensure sequenced, reliable transport of data. The local host and remote host each use these sequence numbers for flow control and to acknowledge receipt of datagrams.

```
iss:   67317172  snduna:   67317228  sndnxt:   67317228     sndwnd:   4096
irs: 1064896000  rcvnxt: 1064897597  rcvwnd:       2144  delrcvwnd:      0
```

Table 117 describes the fields shown in the display.

Table 117 show tcp Field Descriptions—Sequence Number

Field	Description
iss:	Initial send sequence number.
snduna:	Last send sequence number that the local host sent but has not received an acknowledgment for.
sndnxt:	Sequence number the local host will send next.
sndwnd:	TCP window size of the remote host.
irs:	Initial receive sequence number.
rcvnxt:	Last receive sequence number that the local host has acknowledged.
rcvwnd:	TCP window size of the local host.
delrcvwnd:	Delayed receive window—data the local host has read from the connection, but has not yet subtracted from the receive window the host has advertised to the remote host. The value in this field gradually increases until it is larger than a full-sized packet, at which point it is applied to the rcvwnd field.

The following lines of output display values that the local host uses to keep track of transmission times so that TCP can adjust to the network it is using.

```
SRTT: 317 ms, RTTO: 900 ms, RTV: 133 ms, KRTT: 0 ms
minRTT: 4 ms, maxRTT: 300 ms, ACK hold: 300 ms
Flags: higher precedence, idle user, retransmission timeout
```

Table 118 describes the significant fields shown in the output.

Table 118 show tcp Field Descriptions—Line Beginning with "SRTT"

Field	Description
SRTT:	A calculated smoothed round-trip timeout.
RTTO:	Round-trip timeout.
RTV:	Variance of the round-trip time.
KRTT:	New round-trip timeout (using the Karn algorithm). This field separately tracks the round-trip time of packets that have been re-sent.
minRTT:	Smallest recorded round-trip timeout (hard-wire value used for calculation).
maxRTT:	Largest recorded round-trip timeout.
ACK hold:	Time the local host will delay an acknowledgment in order to piggyback data on it.
Flags:	Properties of the connection.

For more information on these fields, refer to *Round Trip Time Estimation*, P. Karn & C. Partridge, ACM SIGCOMM-87, August 1987.

```
Datagrams (max data segment is 536 bytes):
Rcvd: 41 (out of order: 0), with data: 34, total data bytes: 1596
Sent: 57 (retransmit: 1), with data: 35, total data bytes: 55
```

Table 119 describes the significant fields shown in the last lines of the **show tcp** command output.

Table 119 show tcp Field Descriptions—Last Section of Output

Field	Description
Rcvd:	Number of datagrams the local host has received during this connection (and the number of these datagrams that were out of order).
with data:	Number of these datagrams that contained data.
total data bytes:	Total number of bytes of data in these datagrams.
Sent:	Number of datagrams the local host sent during this connection (and the number of these datagrams that needed to be re-sent).
with data:	Number of these datagrams that contained data.
total data bytes:	Total number of bytes of data in these datagrams.

Related Commands

Command	Description
show tcp brief	Displays a concise description of TCP connection endpoints.

show tcp brief

To display a concise description of TCP connection endpoints, use the **show tcp brief** command in EXEC mode.

show tcp brief [**all**]

Syntax Description

all	(Optional) Displays status for all endpoints. Without this keyword, endpoints in the LISTEN state are not shown.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Examples

The following is sample output from the **show tcp brief** command while a user has connected into the system via Telnet:

```
Router> show tcp brief

TCB       Local Address           Foreign Address        (state)
609789AC  Router.cisco.com.23     cider.cisco.com.3733   ESTAB
```

Table 120 describes the significant fields shown in the display.

Table 120 show tcp brief Field Descriptions

Field	Description
TCB	An internal identifier for the endpoint.
Local Address	The local IP address and port.
Foreign Address	The foreign IP address and port (at the opposite end of the connection).
(state)	The state of the connection. States are described in the syntax description of the **show tcp** command.

Related Commands

Command	Description
show tcp	Displays the status of TCP connections.

show tdm connections

To display a snapshot of the time-division multiplexing (TDM) bus connection memory in a Cisco AS5200 access server, use the **show tdm connections** command in EXEC mode.

show tdm connections [**motherboard** | **slot** *slot-number*]

Syntax Description

motherboard	(Optional) Motherboard in the Cisco AS5200 access server.
slot *slot-number*	(Optional) Slot number.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The **show tdm connections** command shows the connection memory for all TDM bus connections in the access server if you do not limit the display to the motherboard or a slot.

Examples

In the following example, source stream 3 (ST3) channel 2 switched out of stream 6 (ST6) channel 2 is shown:

```
AS5200# show tdm connections motherboard

MT8980 motherboard unit 0, Control Register = 0x1F, ODE Register = 0x06
Connection Memory for ST6:
Ch0:  0x62, Ch1:  0x00, Ch2:  0x00, Ch3:  0x00
Ch4:  0x00, Ch5:  0x00, Ch6:  0x00, Ch7:  0x00
Ch8:  0x00, Ch9:  0x00, Ch10: 0x00, Ch11: 0x00
Ch12: 0x00, Ch13: 0x00, Ch14: 0x00, Ch15: 0x00
Ch16: 0x00, Ch17: 0x00, Ch18: 0x00, Ch19: 0x00
Ch20: 0x00, Ch21: 0x00, Ch22: 0x00, Ch23: 0x00
Ch24: 0x00, Ch25: 0x00, Ch26: 0x00, Ch27: 0x00
Ch28: 0x00, Ch29: 0x00, Ch30: 0x00, Ch31: 0x00
```

To interpret the hexadecimal number 0x62 into meaningful information, you must translate it into binary code. These two hexadecimal numbers represent a connection from any stream and a channel on any stream. The number 6 translates into the binary code 0110, which represents the third-source stream. The number 2 translates into the binary code 0010, which represents the second-source channel.

Stream 6 (ST6) channel 0 is the destination for ST3 channel 2 in this example.

Related Commands

Command	Description
show tcp	Displays the status of TCP connections.

show tdm data

To display a snapshot of the time-division multiplexing (TDM) bus data memory in a Cisco AS5200 access server, use the **show tdm data** command in EXEC mode.

show tdm data [**motherboard** | **slot** *slot-number*]

Syntax Description

motherboard	(Optional) Motherboard in the Cisco AS5200 access server.
slot *slot-number*	(Optional) Slot number.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The data memory for all TDM bus connections in the access server is displayed if you do not specify a motherboard or slot.

Examples

In the following example, a snapshot of TDM memory is shown where the normal ISDN idle pattern (0x7E) is present on all channels of the TDM device resident on the motherboard:

```
AS5200# show tdm data motherboard

MT8980 motherboard unit 0, Control Register = 0x1F, ODE Register = 0x06
Data Memory for ST0:
Ch0:  0x7E, Ch1:  0x7E, Ch2:  0x7E, Ch3:  0x7E
Ch4:  0x7E, Ch5:  0x7E, Ch6:  0x7E, Ch7:  0x7E
Ch8:  0x7E, Ch9:  0x7E, Ch10: 0x7E, Ch11: 0x7E
Ch12: 0x7E, Ch13: 0x7E, Ch14: 0x7E, Ch15: 0x7E
Ch16: 0x7E, Ch17: 0x7E, Ch18: 0x7E, Ch19: 0x7E
Ch20: 0x7E, Ch21: 0x7E, Ch22: 0x7E, Ch23: 0x7E
Ch24: 0x7E, Ch25: 0x7E, Ch26: 0x7E, Ch27: 0x7E
Ch28: 0x7E, Ch29: 0x7E, Ch30: 0x7E, Ch31: 0x7E
Data Memory for ST1:
Ch0:  0x7E, Ch1:  0x7E, Ch2:  0x7E, Ch3:  0x7E
Ch4:  0x7E, Ch5:  0x7E, Ch6:  0x7E, Ch7:  0x7E
Ch8:  0x7E, Ch9:  0x7E, Ch10: 0x7E, Ch11: 0x7E
Ch12: 0x7E, Ch13: 0x7E, Ch14: 0x7E, Ch15: 0x7E
Ch16: 0x7E, Ch17: 0x7E, Ch18: 0x7E, Ch19: 0x7E
Ch20: 0x7E, Ch21: 0x7E, Ch22: 0x7E, Ch23: 0x7E
Ch24: 0x7E, Ch25: 0x7E, Ch26: 0x7E, Ch27: 0x7E
Ch28: 0x7E, Ch29: 0x7E, Ch30: 0x7E, Ch31: 0x7E
```

Related Commands

Command	Description
show tdm connections	Displays data about the TDM bus connection memory in a Cisco AS5200 access server.

show tech-support

To display general information about the router when reporting a problem, use the **show tech-support** privileged EXEC command.

show tech-support [**page**] [**password**] [**cef** | **ipmulticast** | **isis** | **mpls** | **ospf** [*process-ID* | **detail**] | **rsvp**]

Syntax Description

page	(Optional) Causes the output to display a page of information at a time. Use the return key to display the next line of output or use the space bar to display the next page of information. If not used, the output scrolls (that is, does not stop for page breaks).
password	(Optional) Leaves passwords and other security information in the output. If not used, passwords and other security-sensitive information in the output are replaced with the label "<removed>" (this is the default).
cef	(Optional) Displays show command output specific to Cisco Express Forwarding (CEF).
ipc	(Optional) Displays show command output specific to Inter-Process Communications (IPC).
ipmulticast	(Optional) Displays show command output related to the IP Multicast configuration, including Protocol Independent Multicast (PIM) information, Internet Group Management Protocol (IGMP) information, and Distance Vector Multicast Routing Protocol (DVMRP) information.
isis	(Optional) Displays show command output specific to Connectionless Network Service (CLNS) and Intermediate System-to-Intermediate System Protocol (ISIS).
mpls	(Optional) Displays show command output specific to Multilayer Switching Protocol (MPLS) forwarding and applications.
ospf [*process-ID* | *detail*]	(Optional) Displays show command output specific to Open Shortest Path First Protocol (OSPF) networking.
rsvp	(Optional) Displays show command output specific to Resource Reservation Protocol (RSVP) networking.

Defaults

The output scrolls without page breaks.
Passwords and other security information are removed from the output.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.

Release	Modification
11.3(7), 11.3(7)T, 11.2(16)	The output for this command was expanded to show additional information for **boot**, **bootflash**, **context**, and **traffic** for all enabled protocols.
12.0	The following keyword extensions were added: • **cef** • **ipmulticast** • **isis** • **mpls** • **ospf**

Usage Guidelines

The **show tech-support** command is useful for collecting a large amount of information about your routing device for troubleshooting purposes. The output of this command can be provided to technical support representatives when reporting a problem.

The **show tech-support** command displays the output of a number of show commands at once. The output from this command will vary depending on your platform and configuration. For example, Access Servers will display voice-related show output. Additionally, the **show** *protocol* **traffic** commands will be displayed for only the protocols enabled on your device. The output of the **show tech-support** command can include the output of the following commands:

- **show apollo traffic**
- **show appletalk traffic**
- **show bootflash**
- **show bootvar**
- **show buffers**
- **show cdp neighbors**
- **show cef**
- **show clns traffic**
- **show context**
- **show controllers**
- **show decnet traffic**
- **show interfaces**
- **show ip cef**
- **show ip interface**
- **show ip traffic**
- **show isis**
- **show mpls**
- **show novell traffic**
- **show processes cpu**
- **show processes memory**
- **show running-config**

- **show stacks**
- **show version**
- **show vines traffic**
- **show xns traffic**
- **show file systems**
- **dir nvram:**
- **show disk0: all**
- **show process cpu**
- **show pci controller**

Use of the optional **cef**, **ipmulticast**, **ipc**, **isis**, **mpls** , **ospf**, or **rsvp** keywords provides a way to display a number of show commands specific to a particular protocol or process in addition to the **show** commands listed previously.

For example, if your TAC support representative suspects that you may have a problem in your Cisco Express Forwarding (CEF) configuration, you may be asked to provide the output of the **show tech-support cef** command. The **show tech-support** [**page**] [**password**] **cef** command will display the output from the following commands in addition to the output for the standard **show tech-support** command:

- **show ip cef summary**
- **show adjacency summary**
- **show ip cef events summary**
- **show ip cef inconsistency records detail**
- **show cef interface**
- **show cef events**
- **show cef timers**
- **show interfaces stats**
- **show cef drop**
- **show cef not-cef-switched**

Examples

For a sample display of the output from the **show tech-support** command, refer to the documentation for the **show** commands listed in the "Usage Guidelines" section.

Related Commands

Command	Description
show apollo traffic	Displays information about the number and type of Apollo Domain packets transmitted and received by the Cisco IOS software.
show appletalk traffic	Displays statistics about AppleTalk traffic, including MacIP traffic.
show bootflash	Displays the contents of boot Flash memory.
show bootvar	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.

Command	Description
show buffers	Displays statistics for the buffer pools on the network server.
show clns traffic	Displays a list of the CLNS packets this router has seen.
show context	Displays context data.
show controllers	Displays information that is specific to the hardware.
show controllers tech-support	Displays general information about a VIP card when reporting a problem.
show decnet traffic	Displays the DECnet traffic statistics (including datagrams sent, received, and forwarded).
show interfaces	Displays ALC information.
show ip traffic	Displays statistics about IP traffic.
show novell traffic	Displays information about the number and type of IPX packets transmitted and received.
show processes cpu	Displays information about the active processes.
show processes memory	Shows the amount of memory used.
show running-config	Displays the current configuration of your routing device.
show stacks	Displays the stack usage of processes and interrupt routines.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.
show vines traffic	Displays the statistics maintained about VINES protocol traffic.
show xns traffic	Displays information about the number and type of XNS packets transmitted and received by the Cisco IOS software.

show version

To display the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images, use the **show version** command in EXEC mode.

show version

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You can also use this command with a Cisco 7507 or Cisco 7513 configured with High System Availability (HSA). HSA refers to how quickly your router returns to an operational status after a failure occurs. On the Cisco 7507 and Cisco 7513, you can install two RSP cards in a single router to improve system availability.

When used with HSA, this command also displays the currently running slave RSP card and the Cisco IOS release that it is running.

Examples

The following is sample output from the **show version** command:

```
Router1> show version

Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-J-M), Experimental Version 11.3(19970915:164752) [
hampton-nitro-baseline 249]
Copyright (c) 1986-1997 by cisco Systems, Inc.
Compiled Wed 08-Oct-97 06:39 by hampton
Image text-base: 0x60008900, data-base: 0x60B98000

ROM: System Bootstrap, Version 11.1(11855) [beta 2], INTERIM SOFTWARE
BOOTFLASH: 7200 Software (C7200-BOOT-M), Version 11.1(472), RELEASE SOFTWARE (fc
1)

Router1 uptime is 23 hours, 33 minutes
System restarted by abort at PC 0x6022322C at 10:50:55 PDT Tue Oct 21 1997
System image file is "tftp://172.16.1.129/hampton/nitro/c7200-j-mz"

cisco 7206 (NPE150) processor with 57344K/8192K bytes of memory.
R4700 processor, Implementation 33, Revision 1.0 (512KB Level 2 Cache)
Last reset from power-on
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
8 Ethernet/IEEE 802.3 interface(s)
2 FastEthernet/IEEE 802.3 interface(s)
```

```
4 Token Ring/IEEE 802.5 interface(s)
4 Serial network interface(s)
1 FDDI network interface(s)
125K bytes of non-volatile configuration memory.
1024K bytes of packet SRAM memory.

20480K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
20480K bytes of Flash PCMCIA card at slot 1 (Sector size 128K).
4096K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x0
```

Table 121 describes the significant fields shown in the display.

Table 121 show version Field Descriptions

Field	Description
IOS (tm) 7200 Software (C7200-J-M), Experimental Version 11.3	Always specify the complete version number when reporting a possible software problem. In the example output, the version number is 11.3.
ROM: System Bootstrap, Version 11.1(11855) [beta 2], INTERIM SOFTWARE	Bootstrap version string.
BOOTFLASH: 7200 Software (C7200-BOOT-M), Version 11.1(472), RELEASE SOFTWARE	Boot version string.
Router1 uptime is	The amount of time the system has been up and running.
System restarted by	Also displayed is a log of how the system was last booted, both as a result of normal system startup and of system error. For example, information can be displayed to indicate a bus error that is generally the result of an attempt to access a nonexistent address, as follows: System restarted by bus error at PC 0xC4CA, address 0x210C0C0.
System image file is	If the software was booted over the network, the Internet address of the boot host is shown. If the software was loaded from onboard ROM, this line reads “running default software.”
cisco 7206 (NPE150) processor	The remaining output in each display shows the hardware configuration and any nonstandard software options.
Configuration register is	The configuration register contents, displayed in hexadecimal notation.

The output of the **show version** EXEC command can also provide certain messages, such as bus error messages. If such error messages appear, report the complete text of this message to your technical support specialist.

The following is sample output from the **show version** command on a Cisco 7500 series router with an RSP2 and three VIP2s with a variety of interfaces:

```
Router# show version

Cisco Internetwork Operating System Software
IOS (tm) GS Software (RSP-JV-M), Experimental Version 11.1(12816)
[getchell 108]
Copyright (c) 1986-1996 by cisco Systems, Inc.
```

```
Compiled Mon 03-Jun-96 11:39 by getchell
Image text-base: 0x600108A0, data-base: 0x60910000

ROM: System Bootstrap, Version 5.3(16645) [szhang 571], INTERIM SOFTWARE

Router uptime is 4 minutes
System restarted by reload
System image file is "slot0:dirt/vip2/master/rsp-jv-mz.960603", booted via tftp from
172.18.2.3

cisco RSP2 (R4600) processor with 24576K bytes of memory.
R4600 processor, Implementation 32, Revision 2.0
Last reset from power-on
G.703/E1 software, Version 1.0.
SuperLAT software copyright 1990 by Meridian Technology Corp).
Bridging software.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
TN3270 Emulation software (copyright 1994 by TGV Inc).
Primary Rate ISDN software, Version 1.0.
Chassis Interface.
1 CIP controller (3 IBM Channels).
1 CIP2 controller (3 IBM Channels).
1 EIP controller (6 Ethernet).
1 HIP controller (1 HSSI).
1 FSIP controller (8 Serial).
1 AIP controller (1 ATM).
1 TRIP controller (4 Token Ring).
1 FIP controller (1 FDDI).
1 MIP controller (2 T1).
3 VIP2 controllers (1 FastEthernet)(13 Ethernet)(4 Serial)(4 Token Ring)(1
Fddi).
1 FEIP controller (1 FastEthernet).
19 Ethernet/IEEE 802.3 interfaces.
2 FastEthernet/IEEE 802.3 interfaces.
8 Token Ring/IEEE 802.5 interfaces.
12 Serial network interfaces.
1 HSSI network interface.
2 FDDI network interfaces.
1 ATM network interface.
2 Channelized T1/PRI ports.
125K bytes of non-volatile configuration memory.

8192K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
8192K bytes of Flash PCMCIA card at slot 1 (Sector size 128K).
8192K bytes of Flash internal SIMM (Sector size 256K).
No slave installed in slot 7.
Configuration register is 0x0
```

Table 122 describes the significant fields shown in the display.

Table 122 show version Field Descriptions on Cisco 7500 Series Routers

Field	Description
IOS (tm) GS Software, Version 11.1	Always specify the complete version number when reporting a possible software problem. In the example output, the version number is 11.1.
ROM: System Bootstrap, Version 5.3(16645) [szhang 571], INTERIM SOFTWARE	Bootstrap version string.

Table 122 show version Field Descriptions on Cisco 7500 Series Routers (continued)

Field	Description
Router uptime is... System restarted by... System image file is...	The amount of time the system has been up and running, how the system was restarted, and the name of the system image file.
System last reset by	Also displayed is a log of how the system was last booted, both as a result of normal system startup and of system error. For example, information can be displayed to indicate a bus error that is generally the result of an attempt to access a nonexistent address, as follows: System restarted by bus error at PC 0xC4CA, address 0x210C0C0.
cisco RSP2 (R4600) processor...	The remaining output in each display shows the software currently running, hardware configuration, and any nonstandard software options. The configuration register contents are displayed in hexadecimal notation.

The following is sample output from the **show version** command for a Cisco 7513 router. In this example, the current slave is processor slot 7:

```
Router# show version

Cisco Internetwork Operating System Software
IOS (tm) GS Software (RSP-P-M), Experimental Version 11.1(5479) [dbath 119]
Copyright (c) 1986-1995 by cisco Systems, Inc.
Compiled Wed 08-Nov-95 17:51 by dbath
Image text-base: 0x600088A0, data-base: 0x603B6000

ROM: System Bootstrap, Version 5.3(18168) [mansonw 63], INTERIM SOFTWARE

Router uptime is 4 days, 31 minutes
System restarted by reload
System image file is "slot0:dirt/dbath/rsp-p-mz-ark-1", booted via tftp from 172.31.7.19


cisco RSP2 (R4600) processor with 16384K bytes of memory.
R4600 processor, Implementation 32, Revision 2.0
Last reset from power-on
G.703/E1 software, Version 1.0.
Primary Rate ISDN software, Version 1.0.
Chassis Interface.
1 CIP controller (3 IBM Channels).
1 CIP2 controller (3 IBM Channels).
1 EIP controller (6 Ethernet).
1 FSIP controller (8 Serial).
1 AIP controller (1 ATM).
1 TRIP controller (4 Token Ring).
1 FIP controller (1 FDDI).
1 MIP controller (2 T1).
6 Ethernet/IEEE 802.3 interfaces.
4 Token Ring/IEEE 802.5 interfaces.
8 Serial network interfaces.
1 FDDI network interface.
1 ATM network interface.
2 Channelized T1/PRI ports.
125K bytes of non-volatile configuration memory.
```

```
8192K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
8192K bytes of Flash internal SIMM (Sector size 256K).

Slave in slot 7 is running Cisco Internetwork Operating System Software
IOS (tm) GS Software (RSP-DW-M), Experimental Version 11.1(5479) [dbath 118]
Copyright (c) 1986-1995 by cisco Systems, Inc.
Compiled Wed 08-Nov-95 16:57 by dbath

Configuration register is 0x0
```

Related Commands

Command	Description
reload	Reloads the operating system.

show whoami

To display information about the terminal line of the current user, including host name, line number, line speed, and location, use the **show whoami** command in EXEC mode.

show whoami [*text*]

Syntax Description

text	(Optional) Additional data to print to the screen.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

If text is included as an argument in the command, that text is displayed as part of the additional data about the line.

To prevent the information from being lost if the menu display clears the screen, this command always displays a --More-- prompt before returning. Press the space bar to return to the prompt.

Examples

The following example is sample output from the **show whoami** command:

```
Router> show whoami


Comm Server "Router", Line 0 at 0bps.  Location "Second floor, West"

--More--
Router>
```

show xsm status

To display information and subscription status of the XML Subscription Manager (XSM) server and clients (such as VPN Device Manager [VDM]), and to display a list of XML data from the XSM server, use the **show xsm status** command in privileged EXEC mode.

show xsm status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use this command to display the following information: which subsystems and histories are enabled or disabled (XSM, Embedded Device Manager [EDM], VDM), XSM client version, number of XSM sessions, duration of XSM session, session IDs, client version and IP address, configuration and monitor privilege levels, and list of subscribed XML Request Descriptors (XRDs).

Examples

The following example shows one XSM session (Session ID = 2) active on the Cisco device for the XSM client at IP address 172.17.129.134, and how long this session has been connected to the XSM server (Session 2: Connected since 22:47:07 UTC Mon Jan 8 2001). The output shows that the XSM, VDM, and EDM subsystems, and EDM and VDM history collecting are enabled. XSM configuration privilege level is set at 15, with XSM monitor privilege level set at 1.

This output also shows the active XRDs (and their version) for Session 2:

```
Router# show xsm status

XSM subsystem is Enabled.
VDM subsystem is Enabled.
EDM subsystem is Enabled.
EDM History is Enabled.
VDM History is Enabled.
XSM privilege configuration level 15.
XSM privilege monitor level 1.

Number of XSM Sessions : 1.

  Session ID = 2.
    XSM Client v0.0(0.0)- @ 172.17.129.134
    Connected since 22:47:07 UTC Mon Jan 8 2001
```

```
List of subscribed xrds:
0 ) device-about                              v1.0
1 ) ios-image                                 v1.0
2 ) if-list                                   v1.0
3 ) device-health                             v1.0
4 ) ike-stats                                 v1.0
5 ) ike                                       v1.0
6 ) ipsec-topn-tunnels-by-traffic             v1.0
7 ) ipsec-topn-tunnels-by-duration            v1.0
8 ) ipsec-stats                               v1.0
9 ) crypto-maps                               v1.0
10) ipsec                                     v1.0
```

Table 123 describes the significant fields shown in the display. (See Table 124 in the documentation of the **show xsm xrd-list** command for a full description of subscribed XRDs).

Table 123 show xsm status Field Descriptions

Field	Description
XSM privilege configuration level	XSM configuration privilege level.
XSM privilege monitor level	XSM monitor privilege level.
Number of XSM Sessions	Total number of concurrent XSM sessions.
Session ID	Specific XSM session number.
XSM Client	Version and IP address of the XSM client.
Connected since	Start time for each session connection to the XSM server.
List of subscribed xrds	Details XRDs available from the XSM server (see **show xsm xrd-list** command for complete list of XRDs).

Related Commands

Command	Description
clear xsm	Clears XSM client sessions.
show xsm xrd-list	Displays all XRDs for clients subscribed to the XSM server.
xsm	Enables XSM client access to the router.
xsm privilege configuration level	Enables configuration privilege level to subscribe to XRDs.
xsm privilege monitor level	Enables monitor privilege level to subscribe to XRDs.

show xsm xrd-list

To display all XML Request Descriptors (XRDs) for XML Subscription Manager (XSM) clients (such as the VPN Device Manager [VDM]) made available by subscription to the XSM server and to identify the required privilege levels, use the **show xsm xrd-list** command in privileged EXEC mode.

show xsm xrd-list

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use this command to display the XRD version and minimum privilege level and type (configuration or monitor) required to view each XRD.

Examples

The following example shows some active XRDs on the XSM server. The end of each line displays the following:

- XRD version number.
- XRD privilege type (configuration or monitor), indicating the privilege level required.

This example displays all available XRDs because both relevant commands (**xsm edm** and **xsm vdm**) have been configured. However, if one command is not configured, only an abbreviated XRD list will appear.

```
Router# show xsm xrd-list
List of all available xrds:
0 ) vlan-db                                 v1.0  privilege=configuration
1 ) entity                                  v1.0  privilege=configuration
2 ) ip                                      v1.0  privilege=configuration
3 ) ios-users                               v1.0  privilege=configuration
4 ) device-about                            v1.0  privilege=monitor
5 ) ios-image                               v1.0  privilege=configuration
6 ) if-stats                                v1.0  privilege=monitor
7 ) if-list                                 v1.0  privilege=configuration
8 ) device-health                           v1.0  privilege=monitor
9 ) time                                    v1.0  privilege=monitor
10) access-lists                            v1.0  privilege=configuration
11) ike-topn-tunnels-by-traffic             v1.0  privilege=monitor
12) ike-topn-tunnels-by-errors              v1.0  privilege=monitor
13) ike-topn-tunnels-by-duration            v1.0  privilege=monitor
14) ike-stats                               v1.0  privilege=monitor
```

```
15) ike                                      v1.0  privilege=configuration
16) certificate-authorities                  v1.0  privilege=configuration
17) ipsec-topn-tunnels-by-traffic            v1.0  privilege=monitor
18) ipsec-topn-tunnels-by-errors             v1.0  privilege=monitor
19) ipsec-topn-tunnels-by-duration           v1.0  privilege=monitor
20) ipsec-stats                              v1.0  privilege=monitor
21) crypto-maps                              v1.0  privilege=configuration
22) ipsec                                    v1.0  privilege=configuration
23) vdm-history                              v1.0  privilege=configuration
24) gre-tunnels                              v1.0  privilege=monitor
end list.
```

Table 124 describes (in alphabetical order) typical XRDs shown in the display.

Table 124 show xsm xrd-list Field Descriptions

Field	Descriptions
access-lists	IOS access control list (ACL) configuration.
certificate-authorities	IOS certificate authority (CA) configuration.
crypto-maps	IOS Crypto Map configuration.
device-about	General network device information.
device-health	General network device health statistics.
edm-history	Selected, historical statistics related to general embedded device management. (This field is not shown in the example above.)
entity	Summary of all physical and logical entities within a device.
gre-tunnels	All current GRE tunnels and respective statistics.
if-list	List of all interfaces and their respective IOS configurations.
if-stats	Statistics for all interfaces and their respective IOS configurations.
ike	IOS Internet Key Exchange (IKE) configuration.
ike-stats	Statistics related to IKE.
ike-topn-tunnels-by-duration	Top 10 IKE tunnels by duration (time).
ike-topn-tunnels-by-errors	Top 10 IKE tunnels by errors.
ike-topn-tunnels-by-traffic	Top 10 IKE tunnels by traffic volume.
ios-image	Information about the current running IOS image.
ios-users	Local IOS user configuration.
ip	IOS IP configuration statistics.
ipsec	IOS IPSec configuration.
ipsec-stats	Interface name and IPSec input and output statistics including: number of packets, dropped packets, octets and errors.
ipsec-topn-tunnels-by-duration	Top 10 IPSec tunnels by duration.
ipsec-topn-tunnels-by-errors	Top 10 IPSec tunnels by errors.
ipsec-topn-tunnels-by-traffic	Top 10 IPSec tunnels by traffic.
time	Device's clock reading in UTC.
vdm-history	Selected, historical VPN-related statistics.

Table 124 show xsm xrd-list Field Descriptions (continued)

Field	Descriptions
vlan-db	VLAN database configuration (switches only).
xsm-session	Status of the current XSM session and related subscriptions. (This field is not shown in the example above.)

Related Commands

Command	Description
clear xsm	Clears XSM client sessions.
show xsm status	Displays information and status about clients subscribed to the XSM server.
xsm	Enables XSM client access to the router.
xsm privilege configuration level	Enables configuration privilege level to subscribe to XRDs.
xsm privilege monitor level	Enables monitor privilege level to subscribe to XRDs.

showmon

To show both the ReadOnly and the Upgrade ROMmon image versions when you are in ROMmon mode, as well as which ROMmon image is running on the Cisco 7200 VXR or Cisco 7301 router, use the **showmon** command in ROMmon mode.

showmon

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

ROMmon

Command History

Release	Modification
12.0(28)S	This command was introduced on the Cisco 7200 VXR router. It was introduced in ROMmon version 12.3(4r)T1 for the Cisco 7200 VXR router.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T and supported on the Cisco 7200 VXR router and Cisco 7301 router. It was introduced in ROMmon version 12.3(4r)T2 for the Cisco 7301 router.
12.3(9)	This command was integrated into Cisco IOS Release 12.3(9) and supported on the Cisco 7200 VXR router and Cisco 7301 router.

Usage Guidelines

Use the **showmon** command when you are in ROMmon mode. Use the **show rom-monitor** command when you are in Cisco IOS.

Examples

The following example, applicable to both the Cisco 7200 VXR and Cisco 7301 routers, uses the **showmon** command in ROMmon to display both ROMmon images and to verify that the Upgrade ROMmon image is running:

```
rommon 1 > showmon

ReadOnly ROMMON version is:
System Bootstrap, Version 12.2(20031011:151758) [biff]
Copyright (c) 2004 by Cisco Systems, Inc.


Upgrade ROMMON version is:
System Bootstrap, Version 12.2(20031011:151758) [biff]
Copyright (c) 2004 by Cisco Systems, Inc.

Upgrade ROMMON currently running
Upgrade ROMMON is selected for next boot
rommon 2 >
```

Related Commands

Command	Description
rommon-pref	Selects a ReadOnly or Upgrade ROMmon image to be booted on the next reload of a Cisco 7200 VXR or Cisco 7301 when you are in ROMmon.

snmp ifmib ifalias long

To configure the system to handle IfAlias descriptions of up to 256 characters, use the **snmp ifmib ifalias long** command in global configuration mode. To limit the IfAlias description to 64 characters, use the **no** form of this command.

snmp ifmib ifalias long

no snmp ifmib ifalias long

Syntax Description

This command has no arguments or keywords.

Defaults

The ifAlias description is limited to 64 characters.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

The ifAlias object (ifXEntry 18) of the Interfaces MIB (IF-MIB) is called the Interface Alias. The Interface Alias (ifAlias) is a user-specified description of an interface used for Simple Network Management Protocol (SNMP) network management. The ifAlias is an object in the Interfaces Group MIB (IF-MIB) which can be set by a network manager to "name" an interface.

The ifAlias value for an interface or subinterface can be set using the **description** command in interface configuration mode or subinterface configuration mode, or by using a Set operation from an NMS. Prior to the introduction of this command, ifAlias descriptions for subinterfaces were limited to 64 characters. (The OLD-CISCO-INTERFACES-MIB allows up to 255 characters for the locIfDescr MIB variable, but this MIB does not support subinterfaces.) IfAlias descriptions appear in the output of the **show interfaces** EXEC mode command, and in the output of the **more system: running-config** or **show running-config** EXEC mode commands.

Examples

In the following example, the system is configured to retain and return ifAlias values of up to 256 characters in length:

```
Router(config)# snmp ifmib ifalias long
```

Related Commands

Command	Description
description	Allows you to specify a description for the specified interface in human-readable form.

Command	Description
show snmp mib	Displays a list of the MIB module instance identifiers (OIDs) registered on your system.
show snmp mib ifmib ifindex	Displays SNMP Interface Index identification numbers (ifIndex values) for all the system interfaces or the specified system interface

snmp mib notification-log default

To create an unnamed Simple Network Management Protocol (SNMP) notification log, use the **snmp mib notification-log default** command in global configuration mode. To delete the log, use the **no** form of this command.

snmp mib notification-log default [**size** *number*]

no snmp mib notification-log default [**size** *number*]

Syntax Description

size *number*	(Optional) Maximum number of entries the log can contain. The default is 500 entries.

Defaults

500 entries

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

This command creates a default unnamed SNMP notification log. The default log has a zero length string as its name (appears in the output of the **show snmp mib notification-log** command as `Log Name"")`.

Creation and removal of the default log can only be performed using the Command Line Interface (CLI). Creation of named logs using the CLI or SNMP tools (SET operations) is not currently supported. No filters (varbinds) can be associated with the default log.

SNMP notification logging is enabled by default, but logging does not start until a specific log is created and defined using this command, or a named log is created using an SNMP Set operation from a network management station (NMS).

The **no** form of this command deletes the default notification log and removes the notifications that were a part of this log from the Notification Log MIB database (recursively deletes the log and all of its entries).

Examples

In the following example, the default SNMP notification log is created and activated, and the log size is set at 600 entries:

```
Router(config)# snmp mib notification-log default size 600
```

Related Commands

Command	Description
show snmp mib notification-log	Displays information about the state of local SNMP notification logging.
snmp mib notification-log globalageout	Sets the maximum age for a notification.
snmp mib notification-log globalsize	Sets the maximum number of notifications allowed in all logs.

snmp mib notification-log default disable

To disable Simple Network Management Protocol (SNMP) notification logging to the "default" log without deleting existing notification log entries, use the **snmp mib notification-log default disable** command in global configuration mode. To reenable logging, use the **no** form of this command.

snmp mib notification-log default disable

no snmp mib notification-log default disable

Syntax Description

This command has no arguments or keywords

Defaults

Logging is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

The "default" notification log is the null-named notification log.

This command disables SNMP notification logging. However, this command does not delete existing logs. To clear the existing "default" log, use the **no snmp mib notification-log default** command.

SNMP notification logging is enabled by default, but logging does not start until a specific log is created and defined using the **snmp mib notification-log default** command, or a named log is created using an SNMP Set operation from a network management station (NMS).

Examples

In the following example, SNMP notification logging is disabled, but existing logs are not deleted:

```
Router(config)# snmp mib notification-log default ?
  disable  disable logging
  size     size of the default log
  <cr>
Router(config)# snmp mib notification-log default disable
Router(config)#
```

Related Commands

Command	Description
show snmp mib notification-log	Displays information about the state of local SNMP notification logging.
snmp mib notification-log default	Creates an SNMP notification log.

Command	Description
snmp mib notification-log globalageout	Sets the maximum age for a notification.
snmp mib notification-log globalsize	Sets the maximum number of notifications allowed in all logs.

snmp mib notification-log globalageout

To set the maximum amount of time Simple Network Management Protocol (SNMP) notification log entries remain in the system memory, use the **snmp mib notification-log globalageout** command in global configuration mode. To restore the default value, use the **no** form of this command.

snmp mib notification-log globalageout *minutes*

no snmp mib notification-log globalageout *minutes*

Syntax Description

minutes	Maximum age (in minutes) that a notification entry is retained in the system memory. The default is 15 minutes.

Defaults

Global Ageout value of 15 minutes

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

The ageout value specifies the maximum time a notification log can remain in the Notification Log MIB database. This value applies to all logs (default log and named logs) in the Notification Log MIB database.

The **no** form of the command restores the default value.

Examples

In the following example, the system is configured to delete entries in the SNMP Notification Log that were logged more than 20 minutes ago:

```
Router(config)# snmp mib notification-log globalageout 20
```

Related Commands

Command	Description
show snmp mib notification-log	Provides a summary of logs.
snmp mib notification-log default	Creates the default log in the MIB.
snmp mib notification-log globalsize	Sets the maximum number of notifications allowed in all logs.

snmp mib notification-log globalsize

To set the maximum number of entries that can be stored in all Simple Network Management Protocol (SNMP) notification Logs, use the **snmp mib notification-log globalsize** command in global configuration mode. To restore the default value, use the **no** form of this command.

snmp mib notification-log globalsize *number*

no snmp mib notification-log globalsize *number*

Syntax Description

number	Maximum number of log entries. The range is from 1 to 15000. This value cannot be set to 0 (limitless). The default is 500.

Defaults

Global log size of 500 entries

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

The size of the SNMP notification log database can be set globally (for all SNMP notification logs combined) or for each named log. The **snmp mib notification-log globalsize** command sets the maximum number of entries for all notification logs on the local system; in other words, this setting affects the whole Notification Log MIB database. This value is saved to the nlmConfigGlobalEntryLimit object in the SNMP Notification Log MIB.

The default global log size is 500 log entries. The default log size for each individual log (such as the “default log”) is 500 log entries. The maximum size for all logs combined is 15,000 log entries.

Examples

In the following example, the system is configured to delete older log entries when there are more than 600 log entries in all SNMP notification logs on the system:

```
Router(config)# snmp mib notification-log globalsize 600
```

Related Commands

Command	Description
show snmp mib notification-log	Provides a summary of logs.
snmp mib notification-log default	Creates the default log in the MIB.
snmp mib notification-log globalageout	Sets the maximum age for a notification.

snmp mib persist

To enable MIB Persistence, use the **snmp mib persist** command in global configuration mode. To disable MIB Persistence, use the **no** form of this command.

snmp mib persist [**event** | **expression** | **circuit**]

no snmp mib persist [**event** | **expression | circuit**]

Syntax Description

event	(Optional) Enables Event MIB Persistence.
expression	(Optional) Enables Expression MIB Persistence.

Defaults

Disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(4)T3	Support for event and expression MIBs was added.

Usage Guidelines

After entering the **snmp mib persist** command, you must enter the **write mib-data** command to save MIB Persistence configuration data to NVRAM.

The Circuit Interface MIB provides a MIB object (cciDescr) that can be used to identify individual circuit-based interfaces for SNMP monitoring. Circuit interface identification persistence maintains the user-defined name of the circuit across reboots by retaining the value of the cciDescr object in the Circuit Interface MIB (CISCO-CIRCUIT-INTERFACE-MIB). A consistent value for specific circuits is useful for network management applications that use SNMP. Circuit interface identification persistence is enabled using the **snmp mib persist circuit** global configuration command. This command is disabled by default because this feature uses NVRAM memory.

To enable both MIB Persistence for all available MIB types, use the **snmp mib persist** command without keywords.

Examples

The following example enables Event MIB Persistence:

```
Router(config)# snmp mib persist event
Router# write mib-data
```

Related Commands

Command	Description
snmp ifindex persist	Enables or disables SNMP interface index values that remain constant across reboots only on a specific interface.
snmp-server ifindex persist	Globally enables SNMP interface index values that remain constant across reboots.
write mib-data	Saves MIB Persistence configuration data to NVRAM.

snmp trap link-status

To enable Simple Network Management Protocol (SNMP) link trap generation, use the **snmp trap link-status** command in interface configuration mode. To disable SNMP link traps, use the **no** form of this command.

snmp trap link-status

no snmp trap link-status

Syntax Description

This command has no arguments or keywords.

Defaults

SNMP link traps are sent when an interface goes up or down.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

By default, SNMP link traps are sent when an interface goes up or down. For interfaces expected to go up and down during normal usage, such as ISDN interfaces, the output generated by these traps may not be useful. The **no** form of this command disables these traps.

Examples

The following example disables the sending of SNMP link traps related to the ISDN BRI 0 interface:

```
interface bri 0
 no snmp trap link-status
```

snmp-server chassis-id

To provide a message line identifying the Simple Network Management Protocol (SNMP) server serial number, use the **snmp-server chassis-id** command in global configuration mode. To restore the default value, if any, use the **no** form of this command.

snmp-server chassis-id *text*

no snmp-server chassis-id

Syntax Description

text	Message you want to enter to identify the chassis serial number.

Defaults

On hardware platforms where the serial number can be machine read, the default is the serial number. For example, a Cisco 7000 router has a default chassis-id value of its serial number.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The Cisco MIB provides a chassis MIB variable that enables the SNMP manager to gather data on system card descriptions, chassis type, chassis hardware version, chassis ID string, software version of ROM monitor, software version of system image in ROM, bytes of processor RAM installed, bytes of NVRAM installed, bytes of NVRAM in use, current configuration register setting, and the value of the configuration register at the next reload. The following installed card information is provided: type of card, serial number, hardware version, software version, and chassis slot number.

The chassis ID message can be seen with the **show snmp** command.

Examples

In the following example, the chassis serial number specified is 1234456:

```
Router(config)# snmp-server chassis-id 1234456
```

Related Commands

Command	Description
show snmp	Checks the status of SNMP communications.

snmp-server community

To set up the community access string to permit access to the Simple Network Management Protocol (SNMP), use the **snmp-server community** command in global configuration mode. To remove the specified community string, use the **no** form of this command.

snmp-server community *string* [**view** *view-name*] [**ro** | **rw**] [*number*]

no snmp-server community *string*

Syntax Description

string	Community string that acts like a password and permits access to the SNMP protocol.
view *view-name*	(Optional) Name of a previously defined view. The view defines the objects available to the community.
ro	(Optional) Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
rw	(Optional) Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.
number	(Optional) Integer from 1 to 99 that specifies an access list of IP addresses that are allowed to use the community string to gain access to the SNMP agent.

Defaults

By default, an SNMP community string permits read-only access to all objects.

Note If the **snmp-server community** command is not used during the SNMP configuration session, it will automatically be added to the configuration after the **snmp host** command is used. In this case, the default password (*string*) for the **snmp-server community** will be taken from the **snmp host** command.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **no snmp-server** command disables all versions of SNMP (SNMPv1, SNMPv2C, SNMPv3).

The first **snmp-server** command that you enter enables all versions of SNMP.

Examples

The following example assigns the string comaccess to SNMP allowing read-only access and specifies that IP access list 4 can use the community string:

```
Router(config)# snmp-server community comaccess ro 4
```

The following example assigns the string mgr to SNMP allowing read-write access to the objects in the restricted view:

```
Router(config)# snmp-server community mgr view restricted rw
```

The following example removes the community comaccess:

```
Router(config)# no snmp-server community comaccess
```

The following example disables all versions of SNMP:

```
Router(config)# no snmp-server
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
snmp-server view	Creates or updates a view entry.

snmp-server contact

To set the system contact (sysContact) string, use the **snmp-server contact** command in global configuration mode. To remove the system contact information, use the **no** form of this command.

snmp-server contact *text*

no snmp-server contact

Syntax Description

text	String that describes the system contact information.

Defaults

No system contact string is set.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is an example of a system contact string:

```
Router(config)# snmp-server contact Dial System Operator at beeper # 27345
```

Related Commands

Command	Description
snmp-server location	Sets the system location string.

snmp-server enable informs

This command has no functionality. To enable the sending of Simple Network Management Protocol (SNMP) inform notifications, use one of the **snmp-server enable traps** *notification-type* commands in global configuration mode combined with the **snmp-server host** *host-address* **informs** commands in global configuration mode.

snmp-server enable traps

To enable all Simple Network Management Protocol (SNMP) notifications (traps or informs) available on your system, use the **snmp-server enable traps** command in global configuration mode. To disable all available SNMP notifications, use the **no** form of this command.

snmp-server enable traps [*notification-type*]

no snmp-server enable traps [*notification-type*]

Syntax Description

notification-type (Optional) Type of notification (trap or inform) to enable or disable. If no type is specified, all notifications available on your device are enabled or disabled. The notification type can be one of the following keywords:

- **config**—Controls configuration notifications, as defined in the CISCO-CONFIG-MAN-MIB (enterprise 1.3.6.1.4.1.9.9.43.2). The notification type is: (1) ciscoConfigManEvent.
- **ds0-busyout**—Sends notification whenever the busyout of a DS0 interface changes state (Cisco AS5300 platform only). This notification is defined in the CISCO-POP-MGMT-MIB (enterprise 1.3.6.1.4.1.9.10.19.2) and the notification type is:(1) cpmDS0BusyoutNotification
- **ds1-loopback**—Sends notification whenever the DS1 interface goes into loopback mode (Cisco AS5300 platform only). This notification type is defined in the CISCO-POP-MGMT-MIB (enterprise 1.3.6.1.4.1.9.10.19.2) as: (2) cpmDS1LoopbackNotification.
- **entity**—Controls Entity MIB modification notifications. This notification type is defined in the ENTITY-MIB (enterprise 1.3.6.1.2.1.47.2) as: (1) entConfigChange.
- **hsrp**—Controls Hot Standby Routing Protocol (HSRP) notifications, as defined in the CISCO-HSRP-MIB (enterprise 1.3.6.1.4.1.9.9.106.2). The notification type is: (1) cHsrpStateChange.**ipmulticast**—Controls IP Multicast notifications.
- **modem-health**—Controls modem-health notifications.
- **rsvp**—Controls Resource Reservation Protocol (RSVP) flow change notifications.
- **tty**—Controls TCP connection notifications.
- **xgcp**—Sends External Media Gateway Control Protocol (XGCP) notifications. This notification is from the XGCP-MIB-V1SMI.my and the notification is enterprise 1.3.6.1.3.90.2 (1) xgcpUpDownNotification

Note For additional notification types, see the Related Commands table.

Defaults

This command is disabled by default. Most notification types are disabled. However, some notification types cannot be controlled with this command.

If you enter this command with no *notification-type* keyword extenstions, the default is to enable (or diable, if the **no** form is used) all notification types controlled by this command.

Command Modes Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(2)T	The **rsvp** keyword was added.
12.0(3)T	The **hsrp** keyword was added.

Usage Guidelines For additional notification types, see the Related Commands table for this command.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. To specify whether the notifications should be sent as traps or informs, use the **snmp-server host** [**traps** | **informs**] command.

If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. In order to configure the router to send these SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled. In order to enable multiple types of notifications, you must issue a separate **snmp-server enable traps** command for each notification type and notification option.

The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.

Examples The following example enables the router to send all traps to the host specified by the name myhost.cisco.com, using the community string defined as public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com public
```

The following example enables the router to send Frame Relay and environmental monitor traps to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps frame-relay
Router(config)# snmp-server enable traps envmon temperature
Router(config)# snmp-server host myhost.cisco.com public
```

The following example will not send traps to any host. The BGP traps are enabled for all hosts, but the only traps enabled to be sent to a host are ISDN traps (which are not enabled in this example).

```
Router(config)# snmp-server enable traps bgp
Router(config)# snmp-server host bob public isdn
```

The following example enables the router to send all inform requests to the host at the address myhost.cisco.com, using the community string defined as public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

The following example sends HSRP MIB traps to the host myhost.cisco.com using the community string public.

```
Router(config)# snmp-server enable traps hsrp
Router(config)# snmp-server host myhost.cisco.com traps version 2c public hsrp
```

Related Commands

Command	Description
snmp-server enable traps atm pvc	Controls (enables or disables) ATM PVC SNMP notifications.
snmp-server enable traps atm pvc extension	Enables the sending of extended ATM permanent virtual circuit (PVC) SNMP notifications.
snmp-server enable traps bgp	Controls (enables or disables) BGP server state change SNMP notifications.
snmp-server enable traps calltracker	Controls (enables or disables) Call Tracker callSetup and callTerminate SNMP notifications.
snmp-server enable traps envmon	Controls (enables or disables) environmental monitor SNMP notifications.
snmp-server enable traps frame-relay	Controls (enables or disables) Frame Relay DLCI link staus change SNMP notifications.
snmp-server enable traps ipsec	Controls (enables or disables) IP Security SNMP notifications.
snmp-server enable traps isakmp	Controls (enables or disables) IPSec Internet Security Association and Key Exchange Protocol (ISAKMP) SNMP notifications.
snmp-server enable traps isdn	Controls (enables or disables) ISDN SNMP notifications.
snmp-server enable traps mpls ldp	Controls (enables or disables) MPLS Label Distribution Protocol (LDP) SNMP notifications.
snmp-server enable traps mpls traffic-eng	Controls (enables or disables) MPLS traffic engineering (TE) tunnel state-change SNMP notifications.
snmp-server enable traps mpls vpn	Controls (enables or disables) MPLS VPN specific SNMP notifications.
snmp-server enable traps repeater	Controls (enables or disables) RFC 1516 Hub notifications.
snmp-server enable traps snmp	Controls (enables or disables) RFC 1157 SNMP notifications.
snmp-server enable traps syslog	Controls (enables or disables) the sending of system logging messages via SNMP.
snmp-server host	Specifies whether you want the SNMP notifications sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the destination host (recipient) for the notifications.
snmp-server informs	Specifies inform request options.
snmp-server trap-source	Specifies the interface (and hence the corresponding IP address) that an SNMP trap should originate from.
snmp trap illegal-address	Issues an SNMP trap when a MAC address violation is detected on an Ethernet hub port of a Cisco 2505, Cisco 2507, or Cisco 2516 router.

snmp-server enable traps aaa_server

To enable authentication, authorization, and accounting (AAA) server state-change Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps aaa_server** command in global configuration mode. To disable AAA server state-change SNMP notifications, use the **no** form of this command.

snmp-server enable traps aaa_server

no snmp-server enable traps aaa_server

Syntax Description

This command has no arguments or keywords.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced for the Cisco AS5300 and Cisco AS5800.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) AAA Server state change (casServerStateChange) notifications. ServerStateChange notifications, when enabled, will be sent when the server moves from an “up” to “dead” state or when a server moves from a “dead” to “up” state.

The Cisco AAA Server State is defined by the casState object in the Cisco AAA Server MIB. The possible values are as follows:

- up(1)—Server is responding to requests.
- dead(2)—Server failed to respond to requests.

A server is marked "dead" if it does not respond after maximum retransmissions. A server is marked "up" again either after a waiting period or if some response is received from it. The initial value of casState is "up(1)" at system startup. This will only transition to "dead(2)" if an attempt to communicate fails.

For a complete description of this notification and additional MIB functions, see the CISCO-AAA-SERVER-MIB.my file, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

The **snmp-server enable traps aaa_sever** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example enables the router to send AAA server up/down informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps aaa_server
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
aaa session-mib disconnect	Allows a remote network management system to perform Set operations and disconnect users on the configured device using SNMP.
show caller	Displays caller information for async, dialer, and serial interfaces.
show radius statistics	Displays AAA server MIB statistics for AAA functions.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps atm pvc extension mibversion

To specify the MIB that supports extended ATM permanent virtual circuit (PVC) Simple Network Management Protocol (SNMP) notifications or the MIB that supports SNMP notifications for ATM Operation, Administration, and Maintenance (OAM) F5 continuity check (CC) management, ATM OAM F5 AIS/RDI management, and F5 loopback failure management, use the **snmp-server enable traps atm pvc extension mibversion** command in global configuration mode. To remove the MIB specification, use the **no** form of this command.

snmp-server enable traps atm pvc extension mibversion {**1** | **2**}

no snmp-server enable traps atm pvc extension mibversion {**1** | **2**}

Syntax Description

1	Specifies the MIB that supports the extended ATM permanent virtual circuit (PVC) SNMP notifications. This is the default.
2	Specifies the MIB that supports ATM OAM F5 CC and ATM OAM F5 AIS/RDI SNMP notifications, in addition to the notifications supported by MIB version 1.

Defaults

MIB version: **1**

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

MIB version 1 specifies the MIB that supports legacy extended ATM PVC traps and is defined in the file CISCO-IETF-ATM2-PVCTRAP-MIB-EXTN.my. MIB version 1 is implemented by default. Use the **snmp-server enable traps atm pvc extension mibversion 1** command or the **no snmp-server enable traps atm pvc extension mibversion 2** command to reenable this MIB if it was previously disabled with the **snmp-server enable traps atm pvc extension mibversion 2** command.

Use the **snmp-server enable traps atm pvc extension mibversion 2** command to specify the MIB that supports ATM OAM F5 CC and ATM OAM AID/RDI failure notifications. This MIB is defined in the file CISCO-ATM-PVCTRAP-EXTN-MIB.my.

To enable the SNMP notifications that support ATM OAM F5 continuity checking, use the **snmp-server enable traps atm pvc extension** command in global configuration mode. These SNMP notifications are defined in the file CISCO-ATM-PVCTRAP-EXTN-MIB.my, available from the Cisco FTP site at ftp://www.cisco.com/public/mibs/v2/.

OAM management and support for OAM F5 continuity checking must be enabled on the PVC by using the **oam-pvc manage cc** command before you can use the ATM OAM continuity check SNMP notifications.

Examples

In the following example, the MIB that supports the SNMP notifications for ATM OAM continuity checking is implemented, and the ATM OAM continuity checking notifications are enabled. Support for end-to-end OAM F5 continuity checking is enabled on PVC 0/1:

```
Router(config)# snmp-server enable traps atm pvc extension mibversion 2
Router(config)# snmp-server enable traps atm pvc extension oam failure aisrdi
Router(config)# snmp-server enable traps atm pvc extension oam failure endcc
Router(config)# snmp-server enable traps atm pvc extension oam failure segmentcc
Router(config)# snmp-server enable traps atm pvc extension oam failure loopback
Router(config)# snmp-server enable traps atm pvc extension up
Router(config)# interface atm 0
Router(config-if)# pvc 0/40
Router(config-if-atm-vc)# oam-pvc manage cc end
```

Related Commands

Command	Description
debug atm oam cc	Displays ATM OAM F5 CC management activity.
oam-pvc manage cc	Configures ATM OAM F5 CC management.
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server enable traps atm pvc	Enables the sending of legacy ATM PVC DOWN traps.
snmp-server enable traps atm pvc extension	Enables the sending of extended ATM PVC SNMP notifications and SNMP notifications for ATM OAM F5 CC, ATM OAM F5 AIS/RDI, and loopback failures.

snmp-server enable traps atm pvc extension

To enable the sending of extended ATM permanent virtual circuit (PVC) SNMP notifications and SNMP notifications for ATM Operation, Administration, and Maintenance (OAM) F5 continuity check (CC), ATM OAM F5 alarm indication signals/remote defect indications (AIS/RDI), and loopback failures, use the **snmp-server enable traps atm pvc extension** command in global configuration mode. To disable these SNMP notifications, use the **no** form of this command.

snmp-server enable traps atm pvc extension {**up** | **down** | **oam failure** [**aisrdi** | **endCC** | **loopback** | **segmentCC**]}

no snmp-server enable traps atm pvc extension{**up** | **down** | **oam failure** [**aisrdi** | **endCC** | **loopback** | **segmentCC**]}

Syntax Description

up	Enables ATM PVC up traps. These notifications are generated when a PVC changes from the DOWN to the UP state.
down	Enables ATM PVC failure traps. These notifications are generated when a PVC changes from the UP to the DOWN state.
oam failure	Enables ATM PVC OAM failure traps. These notifications are generated when any type of OAM failure occurs on the PVC.
aisrdi	(Optional) Enables AIS/RDI OAM failure traps. These notifications are generated when AIS/RDI OAM failure occurs on the PVC.
endCC	(Optional) Enables end-to-end OAM CC failure traps. These notifications are generated when end-to-end CC failures occur on the PVC.
loopback	(Optional) Enables OAM failure loopback traps. These notifications are generated when OAM loopback failure occurs on the PVC.
segmentCC	(Optional) Enables segment OAM CC failure traps. These notifications are generated when segment CC failures occur on the PVC.

Defaults

SNMP notifications are disabled.
The interval between successive traps is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced for those platforms that support ATM PVC management.
12.2(13)T	This command was modified to configure SNMP notification support for ATM OAM F5 CC and ATM OAM F5 AIS/RDI failures.

Usage Guidelines

For PVCs that are not part of a range, extended ATM PVC traps include virtual path identifier/virtual channel indentifier (VPI/ VCI) information, the number of state transitions a PVC goes through in an interval, and the timestamp for the start and end of the transitions. For PVCs that are part of a range, extended ATM PVC traps include the first and last VPI/VCI of the range and the timestamp for the first failure and the last failure within the same range.

Extended ATM PVC and ATM OAM F5 CC traps cannot be used at the same time as the legacy ATM PVC trap. The legacy ATM PVC trap must be disabled by using the **no snmp-server enable traps atm pvc** command before extended ATM PVC traps can be configured.

The extended ATM PVC failure trap (which is is enabled by the **snmp-server enable traps atm pvc extension down** command) is the same trap as the legacy ATM PVC failure trap (which is enabled by the **snmp-server enable traps atm pvc** command), but with the the following differences:

- The extended ATM PVC failure trap contains information in the form of VPI/VCI ranges.
- The extended ATM PVC failure trap contains timestamps for when PVCs go down.
- The legacy ATM PVC failure trap contains only one VPI/VCI per trap.

Note You must configure the **snmp-server enable traps atm pvc extension mibversion 2** command before you can enable the ATM OAM F5 AIS/RDI failure traps, the end-to-end ATM OAM F5 CC failure traps, the OAM failure loopback traps, and the segment ATM OAM F5 CC failure traps. This command enables the MIB that supports these traps.

OAM management must be enabled on the PVC before you can use ATM PVC traps. To generate F5 loopback failure traps, enable OAM management using the **oam-pvc manage** command. To generate segment F5 CC failure traps, enable segment OAM CC management by using the **oam-pvc manage cc segment** command. To generate end-to-end F5 CC failure traps, enable end-to-end OAM CC management by using the **oam-pvc manage cc end** command. To generate OAM F5 AIS/RDI failure traps, enable any of the three types of OAM management listed above.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types.

The extended ATM PVC notifications for MIB version 1 are defined in the CISCO-IETF-ATM2-PVCTRAP-MIB.my file.The extended ATM PVC notifications for MIB version 2 are defined in the CISCO-ATM-PVCTRAP-EXTN-MIB.my file. Both of these MIB files are available from the Cisco FTP site at ftp://www.cisco.com/public/mibs/v2/.

ATM PVC traps are generated at the end of the notification interval. It is possible to generate all three types of ATM PVC traps (the ATM PVC failure trap, ATM PVC up trap, and ATM PVC OAM failure trap) at the end of the same notification interval; however, only one type of trap will be generated for each PVC.

The **snmp-server enable traps atm pvc extension** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.

When the ATM OAM F5 loopback, AIS/RDI, or CC failure trap is enabled, the PVC remains in the UP state when an OAM loopback, AIS/RDI, or CC failure is detected, so that the flow of data will still be possible. If one of these traps is not enabled, the PVC will be placed in the DOWN state when an OAM loopback, AIS/RDI, or CC failure is detected.

Examples

Extended ATM PVC Notifications Example

The following example shows all three of the extended ATM PVC traps enabled on a router. If PVC 0/1 leaves the UP state, leaves the DOWN state, or has an OAM loopback failure, host 172.16.61.90 will receive the SNMP notifications:

```
! Configure SNMP support and an IP routing protocol on your router:
Router(config)# snmp-server community public ro
Router(config)# snmp-server host 172.16.61.90 public
Router(config)# ip routing
Router(config)# router igrp 109
Router(config-router)# network 172.16.0.0
!
! Enable extended ATM PVC trap support and OAM management:
Router(config)# snmp-server enable traps atm pvc extension down
Router(config)# snmp-server enable traps atm pvc extension up
Router(config)# snmp-server enable traps atm pvc extension oam failure loopback
Router(config)# interface atm 1/0.1
Router(config-if)# pvc 0/1
Router(config-if-atm-vc)# oam-pvc manage
```

Extended ATM PVC Failure Trap Output: Example

The following example shows output for extended ATM PVC failure trap for PVCs 1/100, 1/102, and 1/103. Note that only one trap is generated for all the PVCs associated with the same interface or subinterface (in contrast to the legacy ATM PVC failure trap, which generates a separate trap for each PVC). The VPI/VCI information and timing information are located in the objects associated with the trap.

```
00:23:56:SNMP:Queuing packet to 1.1.1.1
00:23:56:SNMP:V2 Trap, reqid 2, errstat 0, erridx 0
sysUpTime.0 = 143636
snmpTrapOID.0 = atmIntfPvcFailuresTrap
ifEntry.1.19 = 19
atmIntfPvcFailures.2 = 7
atmIntfCurrentlyFailingPVcls.2 = 3
atmPVclLowerRangeValue.19.1.2 = 102
atmPVclHigherRangeValue.19.1.2 = 103
atmPVclRangeStatusChangeStart.19.1.2 = 140643
atmPVclRangeStatusChangeEnd.19.1.2 = 140698
atmPVclStatusTransition.19.1.100 = 1
atmPVclStatusChangeStart.19.1.100 = 140636
atmPVclStatusChangeEnd.19.1.100 = 140636
00:23:56:SNMP:Packet sent via UDP to 1.1.1.1
```

Extended ATM PVC Up Trap Output: Example

The following example shows output for the extended ATM PVC up trap for PVCs 1/100, 1/102, and 1/103:

```
00:31:29:SNMP:Queuing packet to 1.1.1.1
00:31:29:SNMP:V2 Trap, reqid 2, errstat 0, erridx 0
sysUpTime.0 = 188990
snmpTrapOID.0 = atmIntfPvcUpTrap
ifEntry.1.19 = 19
atmIntfCurrentlyDownToUpPVcls.2 = 3
atmPVclLowerRangeValue.19.1.2 = 102
atmPVclHigherRangeValue.19.1.2 = 103
atmPVclRangeStatusChangeStart.19.1.2 = 186005
atmPVclRangeStatusChangeEnd.19.1.2 = 186053
atmPVclStatusTransition.19.1.100 = 1
atmPVclStatusChangeStart.19.1.100 = 185990
atmPVclStatusChangeEnd.19.1.100 = 185990
00:31:30:SNMP:Packet sent via UDP to 1.1.1.1
```

ATM OAM F5 CC Notifications Example

In the following example, the ATM OAM CC notifications and an extended ATM PVC notification are enabled. If connectivity failures are detected on PVC 0/1, host 172.16.61.90 will receive the SNMP notifications:

```
! Configure SNMP support and an IP routing protocol on your router:
Router(config)# snmp-server community public ro
Router(config)# snmp-server host 172.16.61.90 public
Router(config)# ip routing
Router(config)# router igrp 109
Router(config-router)# network 172.16.0.0
!
! Enable extended ATM PVC trap support and OAM management:
Router(config)# snmp-server enable traps atm pvc extension mibversion 2
Router(config)# snmp-server enable traps atm pvc extension oam failure aisrdi
Router(config)# snmp-server enable traps atm pvc extension oam failure endcc
Router(config)# snmp-server enable traps atm pvc extension oam failure segmentcc
Router(config)# snmp-server enable traps atm pvc extension oam failure loopback
Router(config)# snmp-server enable traps atm pvc extension up
Router(config)# interface atm 0
Router(config-if)# pvc 0/1
Router(config-if-atm-vc)# oam-pvc manage cc end
```

Related Commands

Command	Description
oam-pvc manage	Enables end-to-end F5 OAM loopback cell generation and OAM management.
oam-pvc manage cc	Configures ATM OAM F5 CC management.
show atm pvc	Displays all ATM PVCs and traffic information.
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server enable traps atm pvc	Enables the sending of legacy ATM PVC failure traps.
snmp-server enable traps atm pvc extension mibversion	Specifies the MIB that supports extended ATM PVC SNMP notifications or the MIB that supports SNMP notifications for ATM OAM F5 CC, F5 AIS/RDI, and F5 loopback failures.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server enable traps atm pvc

To enable the sending of ATM permanent virtual circuit (PVC) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps atm pvc** command in global configuration mode. To disable ATM PVC-specific SNMP notifications, use the **no** form of this command.

snmp-server enable traps atm pvc [**interval** *seconds*] [**fail-interval** *seconds*]

no snmp-server enable traps atm pvc [**interval** *seconds*] [**fail-interval** *seconds*]

Syntax Description

interval *seconds*	(Optional) Minimum period between successive traps, in the range from 1 to 3600. Generation of PVC traps is dampened by the notification interval in order to prevent trap storms. No traps are sent until the interval lapses.
fail-interval *seconds*	(Optional) Minimum period for storing the failed time stamp, in the range from 0 to 3600.

Defaults

SNMP notifications are disabled by default.

The default **interva**l is 30.

The default **fail-interval** is 0.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced for those platforms that support ATM PVC Management.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. ATM notifications are defined in the CISCO-IETF-ATM2-PVCTRAP-MIB.my file, available from the Cisco FTP site at ftp://www.cisco.com/public/mibs/v2/.

ATM PVC failure notification are sent when a PVC on an ATM interface fails or leaves the UP operational state. Only one trap is generated per hardware interface, within the specified interval defined by the **interval** keyword (stored as the atmIntfPvcNotificationInterval in the MIB). If other PVCs on the same interface go DOWN during this interval, traps are generated and held until the **fail-interval** has elapsed. Once the interval has elapsed, the traps are sent if the PVCs are still DOWN.

No notifications are generated when a PVC returns to the UP state after having been in the DOWN state. If you need to detect the recovery of PVCs, you must use the SNMP management application to regularly poll your router.

The **snmp-server enable traps atm pvc** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows the enabling of ATM PVC traps on a router, so that if PVC 0/1 goes down, host 172.16.61.90 will receive the notifications:

```
!For ATM PVC Trap Support to work on your router, you must first have SNMP support and
!an IP routing protocol configured on your router:
Router(config)# snmp-server community public ro
Router(config)# snmp-server host 172.16.61.90 public
Router(config)# ip routing
Router(config)# router igrp 109
Router(config-router)# network 172.16.0.0
!
!Enable ATM PVC Trap Support and OAM management:
Router(config)# snmp-server enable traps atm pvc interval 40 fail-interval 10
Router(config)# interface atm 1/0.1
Router(config-if)# pvc 0/1
Router(config-if-atm-vc)# oam-pvc manage
```

Related Commands

Command	Description
show atm pvc	Displays all ATM permanent virtual circuits (PVCs) and traffic information.
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps atm subif

To enable the sending of ATM subinterface Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps atm subif** command in global configuration mode. To disable ATM subinterface-specific SNMP notifications, use the **no** form of this command.

snmp-server enable traps atm subif [**interval** *seconds* [**count** *number-of-traps*] | [**count** *number-of-traps*]

no snmp-server enable traps atm subif [**interval** *seconds* [**count** *number-of-traps*] | [**count** *number-of-traps*]

Syntax Description

interval *seconds*	(Optional) Minimum period between successive traps, in the range from 0 to 3600. The default is 10 seconds.
count *number-of-traps*	(Optional) Maximum number of traps that will be sent in the specified interval, in the range from 1 to 1000. The default is 10 traps.

Defaults

ATM subinterface SNMP notifications are disabled by default.
Interval: 10 seconds
Count: 10 traps

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types.

ATM subinterface traps are sent to the network management system (NMS) whenever a subinterface enters or leaves the down state.

The **count** and **interval** parameters can be configured to limit the number of traps sent and the frequency at which they are sent in order to prevent trap storms. Configuring an interval of 0 seconds causes all ATM subinterface traps to be sent.

You can disable ATM subinterface traps by using the **no snmp-server enable traps atm subif** command. When traps are disabled, you can use the SNMP management application to poll your router for subinterface status information.

The **snmp-server enable traps atm subif** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.

The **snmp-server trap link ietf** command must be configured in order to use the **snmp-server enable traps atm subif** command. The **snmp-server trap link ietf** command is used to configure your router to use the RFC 2233 IETF standards-based implementation of linkUp/linkDown traps. The default Cisco object definitions do not generate linkUp/linkDown traps correctly for subinterfaces.

Examples

The following example shows how to enable ATM subinterface traps on a router. If an ATM subinterface on this router changes state, host 172.16.61.90 will receive the notifications:

```
!For ATM subinterface trap to work on your router, you must first have SNMP support and
!an IP routing protocol configured on your router:
Router(config)# snmp-server community public ro
Router(config)# snmp-server host 172.16.61.90 public
Router(config)# snmp-server trap link ietf
Router(config)# snmp-server enable traps snmp
Router(config)# ip routing
Router(config)# router igrp 109
Router(config-router)# network 172.16.0.0

!Enable ATM subinterface trap support:
Router(config)# snmp-server enable traps atm subif interval 60 count 5
```

Related Commands

Command	Description
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server enable traps atm pvc	Enables the sending of ATM PVC SNMP notifications.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap link ietf	Enables linkUp/linkDown SNMP traps that are compliant with RFC 2233.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server enable traps bgp

To enable Border Gateway Protocol (BGP) state-change Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps bgp** command in global configuration mode. To disable BGP state-change SNMP notifications, use the no form of this command.

snmp-server enable traps bgp

no snmp-server enable traps bgp

Syntax Description

This command has no arguments or keywords.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced for the Cisco AS5300 and Cisco AS5800.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) BGP server state change notifications, as defined in the BGP4-MIB (enterprise 1.3.6.1.2.1.15.7). The notifications types are:

- bgpEstablished
- bgpBackwardTransition

The BGP notifications are defined in the BGP-4 MIB as follows:

```
bgpTraps                OBJECT IDENTIFIER ::= { bgp 7 }

               bgpEstablished NOTIFICATION-TYPE
                   OBJECTS { bgpPeerLastError,
                             bgpPeerState      }
                   STATUS  current
                   DESCRIPTION
                           "The BGP Established event is generated when
                           the BGP FSM enters the ESTABLISHED state."
                   ::= { bgpTraps 1 }

               bgpBackwardTransition NOTIFICATION-TYPE
                   OBJECTS { bgpPeerLastError,
                             bgpPeerState      }
                   STATUS  current
                   DESCRIPTION
                           "The BGPBackwardTransition Event is generated
                           when the BGP FSM moves from a higher numbered
                           state to a lower numbered state."
                   ::= { bgpTraps 2 }
```

For a complete description of these notifications and additional MIB functions, see the BGP4-MIB.my file, available through the Cisco FTP site at ftp://www.cisco.com/public/mibs/v2/.

Note You may notice incorrect BGP trap OID output when using the SNMP version 1 BGP4-MIB that is available for download at ftp://ftp.cisco.com/pub/mibs/v1/BGP4-MIB-V1SMI.my. When a router sends out BGP traps (notifications) about state changes on an SNMP version 1 monitored BGP peer, the enterprise OID is incorrectly displayed as .1.3.6.1.2.1.15 (bgp) instead of .1.3.6.1.2.1.15.7 (bgpTraps). The problem is not due to any error with Cisco IOS software. This problem occurs because the BGP4-MIB does not follow RFC 1908 rules regarding version 1 and version 2 trap compliance. This MIB is controlled by IANA under the guidance of the IETF, and work is currently in progress by the IETF to replace this MIB with a new version that represents the current state of the BGP protocol. In the meantime, we recommend that you use the SNMP version 2 BGP4-MIB or the CISCO-BGP4-MIB to avoid an incorrect trap OID.

The **snmp-server enable traps bgp** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example enables the router to send BGP state change informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps bgp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps calltracker

To enable Call Tracker CallSetup and Call Terminate Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps calltracker** command in global configuration mode. To disable Call Tracker SNMP notifications, use the **no** form of this command.

snmp-server enable traps calltracker

no snmp-server enable traps calltracker

Syntax Description

This command has no arguments or keywords.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced for the Cisco AS5300 and Cisco AS580 access servers.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) Call Tracker CallSetup and CallTerminate notifications. CallSetup notifications are generated at the start of each call, when an entry is created in the active table (cctActiveTable), and CallTerminate notifications are generated at the end of each call, when an entry is created in the history table (cctHistoryTable).

For a complete description of these notifications and additional MIB functions, refer to the CISCO-CALL-TRACKER-MIB.my file, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

The **snmp-server enable traps calltracker** command is used in conjunction with the **snmp-server host** global configuration command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example enables the router to send call-start and call-stop informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps calltracker
Router(config)# snmp-server host myhost.cisco.com informs version 2c public calltracker
```

Related Commands

Command	Description
calltracker call-record	Enables call record SYSLOG generation for the purpose of debugging, monitoring, or externally saving detailed call record information.
calltracker enable	Enables the Call Tracker feature on an access server.
isdn snmp busyout b-channel	Enables PRI B channels to be busied out via SNMP.
show call calltracker	Displays Call Tracker activity and configuration information such as the number of active calls and the history table attributes.
show modem calltracker	Displays all of the information stored within the Call Tracker Active or History Database for the latest call assigned to specified modem.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps director

To enable DistributedDirector Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps director** command in global configuration mode. To disable DistributedDirector SNMP notifications, use the **no** form of this command.

snmp-server enable traps director [**server-up** | **server-down**]

no snmp-server enable traps director [**server-up** | **server-down**]

Syntax Description

server-up	Enables the DistributedDirector notification that the server has changed to the "up" state.
server-down	Enables the DistributedDirector notification that the server has changed to the "down" state.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) DistributedDirector status notifications for systems. If none of the optional keywords is specified, all available environmental notifications are enabled.

Examples

In the following example, both ciscoDistDirEventServerUp and ciscoDistDirEventServerDown notifications are enabled:

```
Router(config)# snmp-server enable traps director

Router# show running-config

ip host myhost 172.2.2.10 172.2.2.20 172.2.2.30
.
.
.
ip director host myhost
ip dns primary myhost soa myhost myhost@com
ip director host myhost priority boomerang 1
no ip director drp synchronized
snmp-server enable traps director server-up server-down
```

Related Commands

Command	Description
snmp-server enable traps	Enables the router to send SNMP traps.
snmp-server host	Specifies the recipient of an SNMP notification.
snmp-server informs	Specifies inform request options.
snmp-server trap-source	Specifies the interface (and hence the corresponding IP address) from which an SNMP trap should originate.
snmp-server trap-timeout	Defines how often to try resending trap messages on the retransmission queue.
snmp trap link-status	Enables SNMP trap notifications to be generated when a specific port is brought up or down.

snmp-server enable traps dlsw

To enable the sending of Data Link Switch (DLSw) circuit and peer connection Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **snmp-server enable traps dlsw** command in global configuration mode. To disable DLSw notifications, use the **no** form of this command.

snmp-server enable traps dlsw [**circuit** | **tconn**]

no snmp-server enable traps dlsw [**circuit** | **tconn**]

Syntax Description

circuit	(Optional) Enables DLSw circuit traps: • (5) ciscoDlswTrapCircuitUp • (6) ciscoDlswTrapCircuitDown
tconn	(Optional) Enables DLSw peer transport connection traps: • (1) ciscoDlswTrapTConnPartnerReject • (2) ciscoDlswTrapTConnProtViolation • (3) ciscoDlswTrapTConnUp • (4) ciscoDlswTrapTConnDown

Defaults

SNMP notifications are disabled by default.

If the optional keywords are not used, all DLSw notification types are enabled (or disabled, if the **no** form is used).

Command Modes

Global configuration

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests. Use this command in conjunction with the **snmp-server host** command.

This command controls (enables or disables) SNMP notifications for Data Link Switch (DLSw) circuit and connection activity. DLSw objects are defined in the Cisco DLSw MIB module (CISCO-DLSW-MIB.my) and the DLSw+ (Cisco Specific Features) MIB module (CISCO-DLSW-EXT-MIB.my), available through Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Examples

In the following example the device is configured to send DLSw circuit state change informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps dlsw circuit
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps envmon

To enable environmental monitor Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps envmon** command in global configuration mode. To disable environmental monitor SNMP notifications, use the **no** form of this command.

snmp-server enable traps envmon [**shutdown**] [**voltage**] [**temperature**] [**fan**] [**supply**]

no snmp-server enable traps envmon [**shutdown**] [**voltage**] [**temperature**] [**fan**] [**supply**]

Syntax Description

shutdown	(Optional) Controls shutdown notifications. A ciscoEnvMonShutdownNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.1) is sent if the environmental monitor detects a testpoint reaching a critical state and is about to initiate a shutdown.
voltage	(Optional) Controls voltage notifications. A ciscoEnvMonVoltageNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.2) is sent if the voltage measured at a given testpoint is outside the normal range for the testpoint (i.e. is at the warning, critical, or shutdown stage). For access servers, this notification is defined as the caemVoltageNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.61.2.2).
temperature	(Optional) Controls temperature notifications. A ciscoEnvMonTemperatureNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.3) is sent if the temperature measured at a given testpoint is outside the normal range for the testpoint (i.e. is at the warning, critical, or shutdown stage). For access servers, this notification is defined as the caemTemperatureNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.61.2.1).
fan	(Optional) Controls fan failure notifications. A ciscoEnvMonFanNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.4) is sent if any one of the fans in a fan array fails.
supply	(Optional) Controls Redundant Power Supply (RPS) failure notifications. A ciscoEnvMonRedundantSupplyNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.2.5) is sent if a redundant power supply fails.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
11.3(6)AA	Support for this command was introduced for the Cisco AS5300 access server.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) Environmental Monitor (EnvMon) status notifications for supported systems. Cisco enterprise EnvMon notifications are triggered when an environmental threshold is exceeded. If none of the optional keywords are specified, all available environmental notifications are enabled.

For a complete description of these notifications and additional MIB functions, see the CISCO-ENVMON-MIB.my and CISCO-ACCESS-ENVMON-MIB.my files, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

Status of the Environmental Monitor can be viewed using the **show environment** command.

The **snmp-server enable traps envmon** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example enables a Cisco 12000 GSR to send environmental failure informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps envmon
Router(config)# snmp-server host myhost.cisco.com informs version 2c public envmon
```

Related Commands

Command	Description
show environment	Displays environmental conditions on the system.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps frame-relay

To enable Frame Relay Data Link Connection Identifier (DLCI) and subinterface Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps frame-relay** command in global configuration mode. To disable Frame Relay DLCI and subinterface SNMP notifications, use the **no** form of this command.

snmp-server enable traps frame-relay

no snmp-server enable traps frame-relay

Syntax Description

This command has no arguments or keywords.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(13)T	This command was modified to enable Frame Relay subinterface traps in addition to DLCI traps.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) DLCI Frame Relay notifications, as defined in the RFC1315-MIB (enterprise 1.3.6.1.2.1.10.32).

This trap indicates that the indicated virtual circuit (VC) or subinterface has changed state, meaning that the VC or subinterface has either been created or invalidated, or has toggled between the active and inactive states.

To enable only Frame Relay subinterface traps, use the **snmp-server enable traps frame-relay subif** command.

Note For large scale configurations (systems containing hundreds of Frame Relay point-to-point subinterfaces), note that having Frame Relay notifications enabled could potentially have a negative impact on network performance when there are line status changes.

For a complete description of this notification and additional MIB functions, see the RFC1315-MIB.my file and the CISCO-FRAME-RELAY-MIB.my file, available in the “v1” and “v2” directories, respectively, at the Cisco.com MIB web site at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

The **snmp-server enable traps frame-relay** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

In the following example, the router is configured to send Frame Relay DLCI and subinterface state change informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps frame-relay
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps frame-relay subif

To enable Frame Relay subinterface Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps frame-relay subif** command in global configuration mode. To disable Frame Relay subinterface SNMP notifications, use the **no** form of this command.

snmp-server enable traps frame-relay subif [**interval** *seconds* [**count** *number-of-traps*] | [**count** *number-of-traps*]

no snmp-server enable traps frame-relay subif [**interval** *seconds* [**count** *number-of-traps*] | [**count** *number-of-traps*]

Syntax Description

interval *seconds*	(Optional) Minimum period between successive traps, in the range from 0 to 3600. The default is 10 seconds.
count *number-of-traps*	(Optional) Maximum number of traps that will be sent in the specified interval, in the range from 1 to 1000. The default is 10 traps.

Defaults

Frame Relay subinterface SNMP notifications are disabled by default.
Interval: 10 seconds
Count: 10 traps

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

Frame Relay subinterface traps are sent to the network management system (NMS) whenever a subinterface enters or leaves the down state.

The **count** and **interval** parameters can be configured to limit the number of traps sent and the frequency at which they are sent in order to prevent trap storms. Configuring an interval of 0 seconds causes all Frame Relay subinterface traps to be sent.

Note The **snmp-server enable traps frame-relay** command enables both Frame Relay DLCI and subinterface traps. The **snmp-server enable traps frame-relay subif** command enables only Frame Relay subinterface traps.

You can disable Frame Relay subinterface traps by using the **no snmp-server enable traps frame-relay subif** command. When traps are disabled, you can use the SNMP management application to poll your router for subinterface status information.

The **snmp-server enable traps frame-relay subif** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.

The **snmp-server trap link ietf** command must be configured in order to use the **snmp-server enable traps frame-relay subif** command. The **snmp-server trap link ietf** command is used to configure your router to use the RFC 2233 IETF standards-based implementation of linkUp/linkDown traps. The default Cisco object definitions do not generate linkUp/linkDown traps correctly for subinterfaces.

Examples

The following example shows how to enable Frame Relay subinterface traps on a router. If a Frame Relay subinterface on this router changes state, host 172.16.61.90 will receive the notifications:

```
! For Frame Relay subinterface traps to work on your router, you must first have SNMP
! support and an IP routing protocol configured on your router:
Router(config)# snmp-server community public ro
Router(config)# snmp-server host 172.16.61.90 public
Router(config)# snmp-server trap link ietf
Router(config)# snmp-server enable traps snmp
Router(config)# ip routing
Router(config)# router igrp 109
Router(config-router)# network 172.16.0.0

!Enable Frame Relay subinterface trap support:
Router(config)# snmp-server enable traps frame-relay subif interval 60 count 5
```

Related Commands

Command	Description
snmp-server enable traps frame-relay	Enables Frame Relay DLCI link status SNMP notifications.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap link ietf	Enables linkUp/linkDown SNMP traps that are compliant with RFC 2233.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server enable traps isdn

To enable the sending of Integrated Services Digital Network (ISDN) specific Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps isdn** command in global configuration mode. To disable ISDN-specific SNMP notifications, use the **no** form of this command.

snmp-server enable traps isdn [**call-information**] [**chan-not-avail**] [**isdnu-interface**] [**layer2**]

no snmp-server enable traps isdn [**call-information**] [**chan-not-avail**] [**isdnu-interface**] [**layer2**]

Syntax Description

call-information	(Optional) Controls SNMP ISDN call information notifications, as defined in the CISCO-ISDN-MIB (enterprise 1.3.6.1.4.1.9.9.26.2). Notification types are: • demandNbrCallInformation (1) This notification is sent to the manager whenever a successful call clears, or a failed call attempt is determined to have ultimately failed. In the event that call retry is active, then this is after all retry attempts have failed. However, only one such notification is sent in between successful call attempts; subsequent call attempts do not generate notifications of this type. • demandNbrCallDetails (2) This notification is sent to the manager whenever a call connects, or clears, or a failed call attempt is determined to have ultimately failed. In the event that call retry is active, then this is after all retry attempts have failed. However, only one such notification is sent in between successful call attempts; subsequent call attempts do not generate notifications of this type.
chan-not-avail	(Optional) Controls SNMP ISDN channel-not-available notifications. ISDN PRI channel-not-available traps are generated when a requested DS-0 channel is not available, or when there is no modem available to take the incoming call. These notifications are available only for ISDN PRI interfaces.
isdnu-interface	(Optional) Controls SNMP ISDN U interface notifications.
layer2	(Optional) Controls SNMP ISDN layer2 transition notifications.

Defaults

SNMP notifications are disabled by default.

If you enter this command with none of the optional keywords, all available notifications are enabled.

Command Modes

Global configuration

Command History

Release	Modification
10.3	The **snmp-server enable traps isdn** command was introduced.
11.3	The **call-information** and **isdnu-interface** keywords were added for the Cisco 1600 series router.

Release	Modification
12.0	Support for the **call-information** and **isdnu-interface** keywords was introduced for most voice platforms.
12.1(5)T	Support for the **isdn chan-not-available** option was added for the Cisco AS5300, Cisco AS5400, and Cisco AS5800 access servers only.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. ISDN notifications are defined in the CISCO-ISDN-MIB.my and CISCO-ISDNU-IF-MIB.my files, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

Availability of notifications will depend on your platform. To see what notifications are available, use the **snmp-server enable traps isdn ?** command.

If you do not enter an **snmp-server enable traps isdn** command, no notifications controlled by this command are sent. In order to configure the router to send these SNMP notifications, you must enter at least one **snmp-server enable traps isdn** command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.

The **snmp-server enable traps snmp** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows the checking of what notification types are available on a Cisco AS5300, and the enabling of channel-not-available and layer2 informs:

```
NAS(config)#snmp-server enable traps isdn ?
  call-information  Enable SNMP isdn call information traps
  chan-not-avail    Enable SNMP isdn channel not avail traps
  layer2            Enable SNMP isdn layer2 transition traps
  <cr>

NAS(config)#snmp-server enable traps isdn chan-not-avail layer2
NAS(config)#snmp-server host myhost.cisco.com informs version 2c public isdn
```

Related Commands

Command	Description
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server informs	Specifies inform request options.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps mpls ldp

To enable the sending of Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) SNMP notifications, use the **snmp-server enable traps mpls ldp** command in global configuration mode. To disable the sending of MPLS LDP notifications, use the **no** form of this command.

snmp-server enable traps mpls ldp [**session-up** | **session-down** | **pv-limit** | **threshold**]

no snmp-server enable traps mpls ldp [**session-up** | **session-down** | **pv-limit** | **threshold**]

Syntax Description

session-up	(Optional) Controls (enables or disables) LDP session up notifications, defined in the MPLS-LDP-MIB as mplsLdpSessionUp. This notification is generated when the router establishes an LDP session with another LDP entity (an adjacent LDP peer in the network).
session-down	(Optional) Controls (enables or disables) LDP session down notifications, defined in the MPLS-LDP-MIB as mplsLdpSessionDown. This message is generated when an LDP session between the router and its adjacent LDP peer is terminated.
pv-limit	(Optional) Controls (enables or disables) Path-Vector (PV) Limit notifications, defined in the MPLS-LDP-MIB as mplsLdpPVLMismatch. This notification is generated when the router establishes an LDP session with its adjacent peer LSR, but the two LSRs have dissimilar path vector limits.
threshold	(Optional) Controls (enables or disables) PV Limit notifications, defined in the MPLS-LDP-MIB as mplsLdpInitSesThresholdExceeded. This notification is generated after eight failed attempts to establish an LDP session between the router and an LDP peer, due to any type of incompatibility between the devices.

Defaults

The sending of SNMP notifications is disabled by default.

If you do not specify any of the optional keywords, all four types of LDP notifications are enabled on the LSR.

Command Modes

Global configuration

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.2(13)T	This command was implemented in Cisco IOS Release 12.2(13)T.

Usage Guidelines

The MPLS LDP **pv-limit** (mplsLdpPathVectorLimitMismatch) notification object provides a warning message that can be sent to the NMS when two routers engaged in LDP operations have a dissimilar path vector limit. It is recommended that all LDP-enabled routers in the network be configured with the same path vector limit.

The value of the path vector limit can range from 0 through 255; a value of 0 indicates that loop detection is off; any value other than zero up to 255 indicates that loop detection is on and, in addition, specifies the maximum number of hops through which an LDP message can pass before a loop condition in the network is sensed.

The MPLS LDP **threshold** (mplsLdpFailedInitSessionThresholdExceeded) notification object provides a warning message that can be sent to a network management station (NMS) when a local LSR and an adjacent LDP peer attempt to set up an LDP session between them, but fail to do so after a specified number of attempts. The default number of attempts is 8. This default value is implemented in Cisco IOS and cannot be changed using either the CLI or an SNMP agent.

In general, Cisco routers support the same features across multiple platforms. Therefore, the most likely incompatibility to occur between Cisco LSRs is a mismatch of their respective ATM VPI/VCI label ranges.

For example, if you specify a range of valid labels for an LSR that does not overlap the range of its adjacent LDP peer, the routers will try eight times to create an LDP session between themselves before the mplsLdpFailedInitSessionThresholdExceeded notification is generated.

Operationally, the LSRs whose label ranges do not overlap continue their attempt to create an LDP session between themselves after the eight retry threshold is exceeded. In such cases, the LDP threshold exceeded notification alerts the network administrator to the existence of a condition in the network that may warrant attention.

RFC 3036, *LDP Specification*, details the incompatibilities that can exist between Cisco routers and/or other vendor LSRs in an MPLS network. Among such incompatibilities, for example, are the following:

- Non-overlapping ATM VPI/VCI ranges (as noted above) or non-overlapping Frame-Relay DLCI ranges between LSRs attempting to set up an LDP session
- Unsupported label distribution method
- Dissimilar protocol data unit (PDU) size
- Dissimilar LDP feature support

The **snmp-server enable traps mpls ldp** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

In the following example, LDP-specific informs are enabled and will be sent to the host myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps mpls ldp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public mpls-ldp
```

snmp-server enable traps mpls traffic-eng

To enable Multiprotocol Label Switching (MPLS) traffic engineering tunnel state-change SNMP notifications, use the **snmp-server enable traps mpls traffic-eng** command in global configuration mode. To disable MPLS traffic engineering tunnel state-change SNMP notifications, use the **no** form of this command.

snmp-server enable traps mpls traffic-eng [**up** | **down** | **reroute**]

no snmp-server enable traps mpls traffic-eng [**up** | **down** | **reroute**]

Syntax Description

up	(Optional) Enables only mplsTunnelUp notifications { mplsTeNotifyPrefix 1 }. MplsTunnelUp notifications are sent to a network management system (NMS) when an MPLS traffic engineering tunnel is configured and the tunnel transitions from an operationally "down" state to an "up" state.
down	(Optional) Enables only mplsTunnelDown notifications { mplsTeNotifyPrefix 2 }. MplsTunnelDown notifications are generated and sent to the NMS when an MPLS traffic engineering tunnel transitions from an operationally "up" state to a "down" state.
reroute	(Optional) Controls (enables or disables) only mplsTunnelRerouted notifications { mplsTeNotifyPrefix 3 }. MplsTunnelRerouted notifications are sent to the NMS under the following conditions: 1) The signaling path of an existing MPLS traffic engineering tunnel fails for some reason and a new path option is signaled and placed into effect (that is, the tunnel is rerouted). or 2) The signaling path of an existing MPLS traffic engineering tunnel is fully operational, but a better path option can be signaled and placed into effect (that is, the tunnel can be reoptimized). This reoptimization can be triggered by: a) a timer, b) the issuance of an **mpls traffic-eng reoptimize** command, or c) a configuration change that requires the resignaling of a tunnel.

Defaults

SNMP notifications are disabled by default.

If this command is used without keywords, all available trap types (up, down, reroute) are enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.0(17)ST	This command was integrated into Cisco IOS Release 12.0(17)ST.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) MPLS traffic engineering tunnel notifications. MPLS Tunnel StateChange notifications, when enabled, will be sent when the connection moves from an "up" to "down" state, when a connection moves from a "down" to "up" state, or when a connection is rerouted.

If you do not specify a specific argument in conjunction with this command, all three types of MPLS traffic engineering tunnel notifications will be sent.

The **snmp-server enable traps mpls traffic-eng** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example enables the router to send MPLS notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps mpls traffic-eng
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps mpls vpn

To enable the router to send Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) specific Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **snmp-server enable traps mpls vpn** command in global configuration mode. To disable MPLS VPN specific SNMP notifications, use the **no** form of this command.

snmp-server enable traps mpls vpn [**vrf-up**] [**vrf-down**] [**mid-threshold**] [**max-threshold**] [**illegal-label**]

no snmp-server enable traps mpls vpn [**vrf-up**] [**vrf-down**] [**mid-threshold**] [**max-threshold**] [**illegal-label**]

Syntax Description

vrf-up	(Optional) Enables a notification for the assignment of a VRF to an interface that is operational or for the transition of a VRF interface to the operationally up state.
vrf-down	(Optional) Enables a notification for the removal of a VRF from an interface or the transition of an interface to the down state.
mid-threshold	(Optional) Enables a notification of a warning that the number of routes created has crossed the warning threshold. This warning is sent only at the time the warning threshold is exceeded. The warning threshold value is a percentage of the max-threshold value, and is set using the **maximum routes** VRF configuration mode command.
max-threshold	(Optional) Enables a notification that the maximum route limit (maximum route threshold) has been reached. Another notification is sent when the number of routes falls below the maximum route limit value. The max-threshold value is determined by the **maximum routes** VRF configuration mode command.
illegal-label	(Optional) Enables a notification for any illegal labels received on a VRF interface. Labels are illegal if they are outside the legal range, do not have a Label Forwarding Information Base (LFIB) entry, or do not match table IDs for the label.

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

If this command is used without any of the optional keywords, all MPLS VPN notification types are enabled.

For the **vrf-up** (mplsVrfIfUp) or **vrf-down** (mplsVrfIfDown) notifications to be issued from an ATM or Frame Relay subinterface, you must first configure the **snmp-server traps atm subif** command or the **snmp-server traps frame-relay subif** command on the subinterfaces, respectively.

The values for **mid-threshold** and **max-threshold** are set using the **maximum routes** *limit* {*warn-threshold* | **warning-only**} VRF configuration mode command.

The **maximum routes** command gives you two options:

- **maximum routes** *limit* **warning-only**—generate a warning message when the <limit> is exceeded, or
- **maximum routes** *limit warn-threshold*—generate a warning message when the <warn-threshold> is reached.

If you choose **maximum routes** *limit* **warning-only** form of the command, a warning message is generated when the *limit* is exceeded, and the *limit* you specify will not be enforced.

If you choose **maximum routes** *limit warn-threshold* form of the command, a warning message will be generated when the *warn-threshold* is reached, and the *limit* will be enforced.

If you use the **maximum routes** *limit* **warning-only** command with the **snmp-server enable traps mpls vpn** command, a mid-threshold SNMP notification will be generated when the is *limit* value is reached or exceeded.

No max-threshold SNMP notification will be generated.

If you used the **maximum routes** *limit warn-threshold* command with the **snmp-server enable traps mpls vpn** command, a mid-threshold SNMP notification will be generated when the *warn-threshold* value is reached, and a max-threshold notification will be generated when the *limit* value is reached.

The notification types described above are defined in the following MIB objects of the PPVPN-MPLS-VPN-MIB as follows:

- mplsVrfIfUp
- mplsVrfIfDown
- mplsNumVrfRouteMidThreshExceeded
- mplsNumVrfRouteMaxThreshExceeded
- mplsNumVrfSecIllegalLabelThreshExceeded

Examples

In the following example, MPLS VPN trap notifications are sent to the host specified as 172.31.156.34 using the community string named public if a VRF transitions from a down state to an up state or from an up state to a down state:

```
Router(config)# snmp-server enable traps mpls vpn vrf-up vrf-down
Router(config)# snmp-server host 172.31.156.34 traps public mpls-vpn
```

Related Commands

Command	Description
maximum routes	Sets the warning threshold and route maximum for VRFs.
snmp-server enable traps atm subif	Enables ATM Subinterface SNMP notifications.

Command	Description
snmp-server enable traps frame-relay subif	Enables Frame-Relay Subinterface SNMP notifications.
snmp-server host	Specifies the recipient of SNMP notifications.

snmp-server enable traps pim

To enable Protocol Independent Multicast (PIM) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps pim** command in global configuration mode. To disable PIM-specific SNMP notifications, use the **no** form of this command.

snmp-server enable traps pim [**neighbor-change** | **rp-mapping-change** | **invalid-pim-message**]

no snmp-server enable traps pim

Syntax Description

neighbor-change	(Optional) Enables notifications indicating when a router's PIM interface is disabled or enabled, or when a router's PIM neighbor adjacency expires or is established.
rp-mapping-change	(Optional) Enables notifications indicating a change in the rendezvous point (RP) mapping information due to either Auto-RP or bootstrap router (BSR) messages.
invalid-pim-message	(Optional) Enables notifications for monitoring invalid PIM protocol operations (for example, when a router receives a join or prune message for which the RP specified in the packet is not the RP for the multicast group or when a router receives a register message from a multicast group for which it is not the RP).

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. PIM notifications are defined in the CISCO-PIM-MIB.my and PIM-MIB.my files, available from the Cisco MIB web site on Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Examples

The following example shows how to configure a router to generate notifications indicating that a PIM interface of the router has been enabled:

```
! Configure PIM traps to be sent as SNMPv2c traps to host with IP address 10.0.0.1.
Router(config)# snmp-server host 10.0.0.1 traps version 2c public pim

! Configure router to send the neighbor-change class of notifications to host.
Router(config)# snmp-server enable traps pim neighbor-change

! Enable PIM sparse-dense mode on Ethernet interface 0/0.
```

```
Router(config)# interface ethernet0/0
Router(config-if)# ip pim sparse-dense-mode
```

Related Commands

Command	Description
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server enable traps pppoe

To enable Point-to-Point Protocol over Ethernet (PPPoE) session count Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps pppoe** command in global configuration mode. To disable PPPoE session count SNMP notifications, use the **no** form of this command.

snmp-server enable traps pppoe

no snmp-server enable traps pppoe

Syntax Description

This command has no arguments or keywords.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)DC	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

This command enables SNMP traps only. It does not support inform requests.

To configure the PPPoE session-count thresholds at which SNMP notifications will be sent, use the **pppoe limit max-sessions** or **pppoe max-sessions** commands.

For a complete description of this notification and additional MIB functions, see the CISCO-PPPOE-MIB.my file, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

Examples

The following example enables the router to send PPPoE session-count SNMP notifications to the host at the address 10.64.131.20:

```
snmp-server community public RW
snmp-server enable traps pppoe
snmp-server host 10.64.131.20 version 2c public udp-port 1717
```

Related Commands

Command	Description
pppoe limit max-sessions	Sets the maximum number of PPPoE sessions that will be permitted on a router, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.
pppoe max-sessions	Sets the maximum number of PPPoE sessions that will be permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server enable traps repeater

To enable or disable standard repeater (hub) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps repeater** command in global configuration mode. To disable repeater notifications, use the **no** form of this command.

snmp-server enable traps repeater [**health**] [**reset**]

no snmp-server enable traps repeater [**health**] [**reset**]

Syntax Description

health	(Optional) The rptrHealth trap conveys information related to the operational status of the repeater. This trap is sent either when the value of rptrOperStatus changes, or upon completion of a non-disruptive test. The rptrOperStatus object indicates the operational state of the repeater. Status values are as follows: • other(1)—undefined or unknown status • ok(2)—no known failures • rptrFailure(3)—repeater-related failure • groupFailure(4)—group-related failure • portFailure(5)—port-related failure • generalFailure(6)—failure, unspecified type
reset	(Optional) The rptrResetEvent trap is sent on completion of a repeater reset action (triggered by the transition to a START state by a manual command). The rptrResetEvent trap is not sent when the agent restarts and sends an SNMP coldStart or warmStart trap.

Defaults

SNMP notifications are disabled by default.

If no option keywords are specified when entering this command, all repeater notifications available on your system are enabled or disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) Repeater MIB notifications, as defined in RFC 1516. RFC 1516 defines objects for managing IEEE 802.3 10 Mbps baseband repeaters, also known as hubs.

There are two sets of notifications available for this command. The following notification is defined in the CISCO-REPEATER-MIB (enterprise 1.3.6.1.4.1.9.9.22.3):

- 1 ciscoRptrIllegalSrcAddrTrap (illegal source address trap)

The following notifications are defined in the CISCO-REPEATER-MIB-V1SMI (enterprise 1.3.6.1.2.1.22):

- 1 rptrHealth
- 2 rptrGroupChange
- 3 rptrResetEvent

For a complete description of the repeater notifications and additional MIB functions, refer to the CISCO-REPEATER-MIB.my and CISCO-REPEATER-MIB-V1SMI.my files, available on Cisco.com at http://www.cisco.com/public/mibs/.

The **snmp-server enable traps repeater** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example enables the router to send repeater inform notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps repeater
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps rtr

To enable the sending of Service Assurance Agent (SAA) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps rtr** command in global configuration mode. To disable SAA SNMP notifications, use the **no** form of this command.

snmp-server enable traps rtr

no snmp-server enable traps rtr

Syntax Description

This command has no arguments or keywords.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) Cisco Service Assurance Agent notifications, as defined in the Response Time Monitor MIB (CISCO-RTTMON-MIB). The Service Assurance Agent was previously called the Response Time Reporter (RTR); the RTR syntax is retained in this command.

This command enables the following notifications:

- rttMonConnectionChangeNotification—(valid for echo or pathEcho operations only) A rttMonConnectionChangeNotification indicates that a connection to a target (not to a hop along the path to a target) has either failed on establishment or been lost and when reestablished.
- rttMonTimeoutNotification—A rttMonTimeoutNotification indicates the occurrence of a timeout for a SAA operation.
- rttMonThresholdNotification—A rttMonThresholdNotification indicates the occurrence of a threshold violation for a SAA operation.
- rttMonVerifyErrorNotification—A rttMonVerifyErrorNotification indicates the occurrence of data corruption in an SAA operation

For a complete description of these notification types, and for information about the other MIB functions, see the CISCO-RTTMON-MIB.my file, available through the Cisco TAC SNMP Object Navigator tool at http://www.cisco.com/go/mibs . For further information about the SAA, see the *Network Monitoring Using the Cisco Service Assurance Agent* document at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcfprt3/fcf017.htm.

The **snmp-server enable traps syslog** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example enables the router to send SAA related informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps rtr
Router(config)# snmp-server host myhost.cisco.com informs version 2c public rtr
```

Related Commands

Command	Description
rtr	Assigns an identification number for an SAA operation and enters SAA RTR configuration mode.
snmp-server host	Specifies the destination NMS and transfer parameters for SNMP notifications.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps snmp

To enable the sending of RFC 1157 Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps snmp** command in global configuration mode. To disable RFC 1157 SNMP notifications, use the **no** form of this command.

snmp-server enable traps snmp [**authentication**] [**linkup**] [**linkdown**] [**coldstart**] [**warmstart**]

no snmp-server enable traps snmp [**authentication**] [**linkup**] [**linkdown**] [**coldstart**] [**warmstart**]

Syntax Description

authentication	(Optional) Controls the sending of SNMP authentication failure notifications. An authenticationFailure(4) trap signifies that the sending device is the addressee of a protocol message that is not properly authenticated. The authentication method depends on the version of SNMP being used. For SNMPv1 or SNMPv2c, authentication failure occurs for packets with an incorrect community string. For SNMPv3, authentication failure occurs for packets with an incorrect SHA/MD5 authentication key or for a packet that is outside of the authoritative SNMP engine's window (for example, falls outside of configured access lists or time ranges).
linkup	(Optional) Controls the sending of SNMP linkUp notifications. A linkUp(3) trap signifies that the sending device recognizes that one of the communication links represented in the agent's configuration has come up.
linden	(Optional) Controls the sending of SNMP linkDown notifications. A linkDown(2) trap signifies that the sending device recognizes a failure in one of the communication links represented in the agent's configuration.
coldstart	(Optional) Controls the sending of SNMP coldStart notifications. A coldStart(0) trap signifies that the sending device is reinitializing itself such that the agent's configuration or the protocol entity implementation may be altered.
warmstart	(Optional) Controls the sending of SNMP warmStart notifications. A warmStart(1) trap signifies that the sending device is reinitializing itself such that neither the agent configuration nor the protocol entity implementation is altered.

Defaults

SNMP notifications are disabled by default.

If you enter this command with none of the optional keywords, all RFC 1157 SNMP notifications are enabled (or disabled, if using the **no** form).

Command Modes

Global configuration

Command History

Release	Modification
11.3	The **snmp-server enable traps snmp authentication** command was introduced. This command replaced the **snmp-server trap-authentication** command.
12.1(3)T	The following keywords were added: • **linkup** • **linkdown** • **coldstart**
12.1(5)T	The **warmstart** keyword was added.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types.

If you do not enter an **snmp-server enable traps snmp** command, no notifications controlled by this command are sent. In order to configure the router to send these SNMP notifications, you must enter at least one **snmp-server enable traps snmp** command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.

The **snmp-server enable traps snmp** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.

For a host to receive a notification controlled by this command, both the **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled. If the notification type is not controlled by this command, just the appropriate **snmp-server host** command must be enabled.

The **snmp-server enable traps snmp** [**linkup**] [**linkdown**] form of this command globally enables or disables SNMP linkUp and linkDown traps. After enabling either of these traps globally, you can disable these traps on specific interfaces using the **no snmp trap link-status** command in interface configuration mode. Note that on the interface level, linkUp and linkDown traps are enabled by default. This means that you do not have to enable these notifications on a per-interface basis. However, linkUp and linkDown notifications will not be sent unless you enable them globally using the **snmp-server enable traps snmp** command.

Examples

The following example enables the router to send all traps to the host `myhost.cisco.com`, using the community string defined as `public`:

```
Router(config)# snmp-server enable traps snmp
Router(config)# snmp-server host myhost.cisco.com public snmp
```

The following example enables the router to send all inform notifications to the host `myhost.cisco.com` using the community string defined as `public`:

```
Router(config)# snmp-server enable traps snmp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public snmp
```

The following example shows the enabling all SNMP trap types, then the disabling of only the linkUp and linkDown trap:

```
Router> enable
Password:
Router# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# snmp-server enable traps snmp
Router(config)# end
Router# more system:running-config | include traps snmp
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no snmp-server enable traps snmp linkup linkdown
Router(config)# end
Router# more system:running-config | include traps snmp
snmp-server enable traps snmp authentication coldstart warmstart
```

Related Commands

Command	Description
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server informs	Specifies inform request options.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps srp

To enable the sending of Intelligent Protection Switching (IPS) Spatial Reuse Protocol (SRP) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps srp** command in global configuration mode. To disable SRP notifications, use the **no** form of this command.

snmp-server enable traps srp

no snmp-server enable traps srp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced to support DPT-OC12 Port Adapters.

Usage Guidelines

The Cisco SRP MIB module (CISCO-SRP-MIB.my) provides objects for monitoring IP-over-SONET IPS SRP traffic using the SNMP. When IPS is enabled, if a node or fiber facility failure is detected, traffic going toward or coming from the failure direction is wrapped (looped) back to go in opposite direction on the other ring.

The **snmp-server enable traps srp** command enables SRP state change notifications (traps or informs). SRP state change notifications are generated whenever one of the two sides of an SRP interface ring enters or leaves the wrapped state (when a ring wraps, or when a ring is restored).

Specifically, the srpMACIpsWrapCounter object in the CISCO-SRP-MIB increments when a Ring wraps, and the value of the rpMACIpsLastUnWrapTimeStamp object changes when a ring unwraps. (An "unwrap" event happens when the original ring is restored.)

The **snmp-server enable traps srp** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

In the following example, SRP-specific informs are enabled and will be sent to the host "myhost.cisco.com" using the community string defined as public:

```
Router(config)# snmp-server enable traps srp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public srp
```

snmp-server enable traps syslog

To enable the sending of system logging message Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps syslog** command in global configuration mode. To disable system logging message SNMP notifications, use the **no** form of this command.

snmp-server enable traps syslog

no snmp-server enable traps syslog

Syntax Description

This command has no arguments or keywords.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) system logging message notifications. System logging messages (also called system error messages, or syslog messages) are status notification messages that are generated by the routing device during operation. These messages are typically logged to a destination (such as the terminal screen, to a system buffer, or to a remote “syslog” host).

If your software image supports the Cisco Syslog MIB, these messages can also be sent via SNMP to a network management station (NMS). To determine which software images support the Cisco Syslog MIB, used the Cisco MIB Locator tool at http://www.cisco.com/go/mibs/ .(At the time of writing, the Cisco Syslog MIB is only supported in “Enterprise” images.)

Unlike other logging processes on the system, debug messages (enabled using CLI debug commands) are not included with the logging messages sent via SNMP.

To specify the severity level at which notifications should be generated, use the **logging history** global configuration command. For additional information about the system logging process and severity levels, see the description of the **logging** commands.

The syslog notification is defined by the clogMessageGenerated NOTIFICATION-TYPE object in the Cisco Syslog MIB (CISCO-SYSLOG-MIB.my). When a syslog message is generated by the device a clogMessageGenerated notification is sent to the designated NMS. The clogMessageGenerated notification includes the following objects: clogHistFacility, clogHistSeverity, clogHistMsgName, clogHistMsgText, clogHistTimestamp.

For a complete description of these objects and additional MIB information, see the text of CISCO-SYSLOG-MIB.my, available on Cisco.com using the SNMP Object Navigator tool at http://www.cisco.com/go/mibs . See also the CISCO-SYSLOG-EXT-MIB and the CISCO-SYSLOG-EVENT-EXT-MIB.

The **snmp-server enable traps syslog** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example enables the router to send system logging messages at severity levels 0 (emergencies) through 2 (critical) to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps syslog
Router(config)# logging history 2
Router(config)# snmp-server host myhost.cisco.com traps version 2c public
```

Related Commands

Command	Description
logging history	Limits syslog messages sent to the router's history table and to an SNMP NMS based on severity.
snmp-server host	Specifies the destination NMS and transfer parameters for SNMP notifications.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps voice poor-qov

To enable poor quality of voice Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps voice poor-qov** command in global configuration mode. To disable poor quality of voice SNMP notifications, use the **no** form of this command.

snmp-server enable traps voice poor-qov

no snmp-server enable traps voice poor-qov

Syntax Description

This command has no arguments or keywords.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced for the Cisco AS5300 and Cisco AS5800.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) poor-quality-of-voice notifications. The poor-quality-of-voice notification is defined in CISCO-VOICE-DIAL-CONTROL-MIB as follows:

enterprise 1.3.6.1.4.1.9.9.63.2

(1) cvdcPoorQoVNotification

For a complete description of this notification and additional MIB functions, see the CISCO-VOICE-DIAL-CONTROL-MIB.my file, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

The **snmp-server enable traps voice poor-qov** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example enables the router to poor-quality-of-voice informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps voice poor-qov
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server engineID local

To specify the Simple Network Management Protocol (SNMP) engine ID on the local device, use the **snmp-server engineID local** command in global configuration mode. To remove the configured engine ID, use the **no** form of this command.

snmp-server engineID local *engineid-string*

no snmp-server engineID local *engineid-string*

Syntax Description

engineid-string	The character string that identifies the engine ID. Consists of up to 24 characters.

Defaults

An SNMP engine ID is generated automatically but is not displayed or stored in the running configuration. You can display the default or configured engine ID by using the **show snmp engineID** EXEC command.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

The SNMP engine ID is a unique string used to identify the device for administration purposes. You do not need to specify an engine ID for the device; a default string is generated using Cisco's enterprise number (1.3.6.1.4.1.9) and the mac address of the first interface on the device. For further details on the SNMP engine ID, see RFC 2571.

If you wish to specify your own ID, note that you need not specify the entire 24-character engine ID if it contains trailing zeros. Specify only the portion of the Engine ID up until the point where only zeros remain in the value. For example, to configure an engine ID of 123400000000000000000000, you can specify **snmp-server engineID local 1234**.

Changing the value of snmpEngineID has important side-effects. A user's password (entered on the command line) is converted to an MD5 or SHA security digest. This digest is based on both the password and the local engine ID. The command line password is then destroyed, as required by RFC 2274. Because of this deletion, if the local value of engineID changes, the security digests of SNMPv3 users will be invalid, and the users will have to be reconfigured.

Similar restrictions require the reconfiguration of community strings when the engine ID changes. A remote engine ID is required when an SNMPv3 inform is configured. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

Related Commands

Command	Description
show snmp engineID	Displays the identification of the local SNMP engine and all remote engines that have been configured on the router.
snmp-server host	Specifies the recipient (SNMP manager) of an SNMP trap notification.

snmp-server engineID remote

To specify the Simple Network Management Protocol (SNMP) engine ID of a remote SNMP device, use the **snmp-server engineID remote** command in global configuration mode. To remove the configured engine ID, use the **no** form of this command.

snmp-server engineID remote *ip-address* [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] *engineid-string*

no snmp-server engineID remote *ip-address* [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] *engineid-string*

Syntax Description

ip-address	The IP address of the device that contains the remote copy of SNMP.
udp-port	(Optional) Specifies a User Datagram Protocol (UDP) port of the host to use.
udp-port-number	(Optional) The socket number on the remote device that contains the remote copy of SNMP. The default is 161.
vrf	(Optional) Instance of a routing table.
vrf-name	(Optional) Name of the VPN routing/forwarding (VRF) table to use for storing data.
engineid-string	The character string that identifies the engine ID. Consists of up to 24 characters.

Defaults

UDP port: 161

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(2)T	The **vrf** keyword and *vrf-name* argument were introduced.

Usage Guidelines

You need not specify the entire 24-character engine ID if it contains trailing zeros. Specify only the portion of the engine ID up until the point where only zeros remain in the value. For example, to configure an engine ID of 123400000000000000000000, you can specify the value 1234 as the *engineid-string*.

A remote engine ID is required when an SNMP version 3 inform is configured. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

Examples

The following example specifies the SNMP engine ID and configures the VRF name traps-vrf for SNMP communications with the remote device at 172.16.20.3:

```
Router(config)# snmp-server engineID remote 172.16.20.3 vrf traps-vrf
80000009030000B064EFE100
```

Related Commands

Command	Description
show snmp engineID	Displays the identification of the local SNMP engine and all remote engines that have been configured on the router.
snmp-server host	Specifies the recipient (SNMP manager) of an SNMP trap notification.

snmp-server group

To configure a new Simple Network Management Protocol (SNMP) group, or a table that maps SNMP users to SNMP views, use the **snmp-server group** command in global configuration mode. To remove a specified SNMP group, use the **no** form of this command.

snmp-server group *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** *access-list*]

no snmp-server group

Syntax Description

group-name	The name of the group.
v1	The least secure of the possible security models.
v2c	The second least secure of the possible security models. It allows for the transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.
v3	The most secure of the possible security models.
auth	Specifies authentication of a packet without encrypting it.
noauth	Specifies no authentication of a packet.
priv	Specifies authentication of a packet with encryption.
read	(Optional) The option that allows you to specify a read view.
read-view	A string (not to exceed 64 characters) that is the name of the view that enables you only to view the contents of the agent.
write	(Optional) The option that allows you to specify a write view.
write-view	A string (not to exceed 64 characters) that is the name of the view that enables you to enter data and configure the contents of the agent.
notify	(Optional) The option that allows you to specify a notify view
notify-view	A string (not to exceed 64 characters) that is the name of the view that enables you to specify a notify, inform, or trap.
access	(Optional) The option that enables you to specify an access list.
access-list	A string (not to exceed 64 characters) that is the name of the access list.

Defaults

Table 125 describes default values for the different views.

Table 125 snmp-server group Default Descriptions

Default	Definition
read-view	Assumed to be every object belonging to the Internet (1.3.6.1) OID space, unless the user uses the read option to override this state.

Table 125 snmp-server group Default Descriptions (continued)

Default	Definition
write-view	Nothing is defined for the write view (that is, the null OID). You must configure write access.
notify-view	Nothing is defined for the notify view (that is, the null OID). If a view is specified, any notifications in that view that are generated will be sent to all users associated with the group (provided an SNMP server host configuration exists for the user).

Command Modes

Global configuration

Command History

Release	Modification
11.(3)T	This command was introduced.

Usage Guidelines

When a community string is configured internally, two groups with the name public are autogenerated, one for the v1 security model and the other for the v2c security model. Similarly, deleting a community string will delete a v1 group with the name public and a v2c group with the name public.

Configuring Notify Views

Do not specify a notify view when configuring an SNMP group for the following reasons:

- The **snmp-server host** command autogenerates a notify view for the user, and then adds it to the group associated with that user.
- Modifying the group's notify view will affect all users associated with that group.

The *notifyview* option is available for two reasons:

- If a group has a notify view that is set using SNMP, you may need to change the notify view.
- The **snmp-server host** command may have been configured before the **snmp-server group** command. In this case, you must either reconfigure the **snmp-server host** command, or specify the appropriate notify view.

Instead of specifying the notify view for a group as part of the **snmp-server group** command, use the following commands in global configuration mode:

	Command	Purpose
Step 1	**snmp-server user**	Configures an SNMP user.
Step 1	**snmp-server group**	Configures an SNMP group, without adding a notify view.
Step 1	**snmp-server host**	Autogenerates the notify view by specifying the recipient of a trap operation.

Working with Passwords and Digests

No default values exist for authentication or privacy algorithms when you configure the command. Also, no default passwords exist. The minimum length for a password is one character, although Cisco recommends using eight characters for security. If you forget a password, you cannot recover it and will need to reconfigure the user. You can specify either a plain-text password or a localized MD5 digest.

The following example shows how to enter a plain-text password for the string arizona2 for user John in group Johngroup, type the following command line:

```
snmp-server user John Johngroup v3 auth md5 arizona2
```

When you enter a **show running-config** command, you will not see a line for this user. To see if this user has been added to the configuration, type the **show snmp user** command.

If you have the localized MD5 or SHA digest, you can specify that string instead of the plain-text password. The digest should be formatted as aa:bb:cc:dd where aa, bb, and cc are hex values. Also, the digest should be exactly 16 octets long.

The following example shows how to specify the command with a digest name of 00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF:

```
Router(config)# snmp-server user John Johngroup v3 encrypted auth md5
00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF
```

Related Commands

Command	Description
show snmp group	Displays the names of groups on the router and the security model, the status of the different views, and the storage type of each group.

snmp-server host

To specify the recipient of an Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** command in global configuration mode. To remove the specified host from the configuration, use the **no** form of this command.

snmp-server host *host-address* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] *[notification-type*] [**vrf** *vrf-name*]

no snmp-server host *host-address* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] *[notification-type*] [**vrf** *vrf-name*]

Syntax Description

host-address	Name or Internet address of the host (the targeted recipient).
traps	(Optional) Specifies that notifications should be sent as traps. This is the default.
informs	(Optional) Specifies that notifications should be sent as informs.
version	(Optional) Version of the SNMP used to send the traps. Version 3 is the most secure model, because it allows packet encryption with the **priv** keyword. If you use the **version** keyword, one of the following keywords must be specified: • **1** —SNMPv1. This option is not available with informs. • **2c** —SNMPv2C. • **3** —SNMPv3. One of the following three optional keywords can follow the version 3 keyword: – **auth**—Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication – **noauth**—Specifies that the noAuthNoPriv security level applies to this host. This is the default security level for SNMPv3. – **priv**—Enables Data Encryption Standard (DES) packet encryption (also called “privacy”).
community-string	Password-like community string sent with the notification operation. Though you can set this string using the **snmp-server host** command by itself, we recommend you define this string using the **snmp-server community** command prior to using the **snmp-server host** command.
udp-port *port*	(Optional) User Datagram Protocol (UDP) port of the host to use. The default is 162.

notification-type (Optional) Type of notification to be sent to the host. If no type is specified, all available notifications are sent. The notification type can be one or more of the following keywords:

- **bgp**—Sends Border Gateway Protocol (BGP) state change notifications.
- **calltracker**—Sends Call Tracker call-start/call-end notifications.
- **config**—Sends configuration change notifications.
- **director**—Sends DistributedDirector-related notifications.
- **dspu**—Sends downstream physical unit (DSPU) notifications.
- **entity**—Sends Entity MIB modification notifications.
- **envmon**—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded.
- **frame-relay**—Sends Frame Relay notifications.
- **hsrp**—Sends Hot Standby Routing Protocol (HSRP) notifications.
- **ipmobile**—Sends Mobile IP notifications.
- **ipsec**—Sends IP Security (IPSec) notifications.
- **isdn**—Sends ISDN notifications.
- **llc2**—Sends Logical Link Control, type 2 (LLC2) notifications.
- **mpls-ldp**—Sends MPLS Label Distribution Protocol (LDP) notifications indicating status changes in LDP sessions.
- **mpls-traffic-eng**—Sends MPLS traffic engineering notifications indicating changes in the status of MPLS traffic engineering tunnels.
- **mpls-vpn**—Sends MPLS VPN notifications.
- **pim**—Sends Protocol Independent Multicast (PIM) notifications.
- **repeater**—Sends standard repeater (hub) notifications.
- **rsrb**—Sends remote source-route bridging (RSRB) notifications.
- **rsvp**—Sends Resource Reservation Protocol (RSVP) notifications.
- **rtr**—Sends Service Assurance Agent (RTR) notifications.
- **sdlc**—Sends Synchronous Data Link Control (SDLC) notifications.
- **sdllc**—Sends SDLC Logical Link Control (SDLLC) notifications.
- **snmp**—Sends any enabled RFC 1157 SNMP linkUp, linkDown, authenticationFailure, warmStart, and coldStart notifications.

Note To enable RFC 2233 compliant link up/down notifications, you should use the **snmp server link trap** command.

- **srp**—Sends Spatial Reuse Protocol (SRP) notifications.
- **stun**—Sends serial tunnel (STUN) notifications.
- **syslog**—Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the **logging history level** command.

notification-type (Continued)	• **tty**—Sends Cisco enterprise-specific notifications when a TCP connection closes. • **voice**—Sends SNMP poor quality of voice traps, when used with the **snmp enable peer-trap poor qov** command. • **vsimaster—**Sends VSI Master notifications. • **x25**—Sends X.25 event notifications.
vrf *vrf-name*	(Optional) Specifies the Virtual Private Network (VPN) routing and forwarding (VRF) table that should be used to send SNMP notifications.

Defaults

This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs will be sent to this host.

If no **version** keyword is present, the default is version 1. If version 3 is specified, but the security level is not specified, the default security level is **noauth**.

The **no snmp-server host** command with no keywords will disable traps, but not informs, to the host. In order to disable informs, use the **no snmp-server host informs** command.

The default UDP port is 162.

Note If the *community-string* is not defined using the **snmp-server community** command prior to using this command, the default form of the **snmp-server community** command will automatically be inserted into the configuration. The password (*community-string*) used for this automatic configuration of the **snmp-server community** will be the same as specified in the **snmp-server host** command. This is the default behavior for Cisco IOS Release 12.0(3) and later.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(3)T	The following keywords were added: • **version 3** [**auth** | **noauth** | **priv**] • **hsrp**
11.3(1) MA, 12.0(3)T	The **voice** notification-type keyword was added.
12.1(3)T	The **calltracker** notification-type keyword was added for the Cisco AS5300 and AS5800 platforms.
12.2(2)T	• The **vrf** *vrf-name* keyword/argument combination was added. • The **ipmobile** notification-type keyword was added. • Support for the **vsimaster** notification-type keyword was added for the Cisco 7200 and Cisco 7500 series.
12.2(4)T	• The **pim** notification-type keyword was added. • The **ipsec** notification-type keyword was added.

Release	Modification
12.2(8)T	• The **mpls-traffic-eng** notification-type keyword was added. (Also in 12.0(17)ST) • The **director** notification-type keyword was added.
12.2(13)T	• The **srp** notification-type keyword was added. • The **mpls-vpn** notification-type keyword was added. (Also in 12.0(22)S) • The **mpls-ldp** notification-type keyword was added.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once, while an inform may be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. In order to configure the router to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host.

In order to enable multiple hosts, you must issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command will be in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command will replace the first.

The **snmp-server host** command is used in conjunction with the **snmp-server enable** command. Use the **snmp-server enable** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

However, some notification types cannot be controlled with the **snmp-server enable** command. For example, some notification types are always enabled. Other notification types are enabled by a different command. For example, the linkUpDown notifications are controlled by the **snmp trap link-status** command. These notification types do not require an **snmp-server enable** command.

A notification-type option's availability depends on the router type and Cisco IOS software features supported on the router. For example, the **envmon** notification-type is available only if the environmental monitor is part of the system. To see what notification types are available on your system, use the command help **?** at the end of the **snmp-server host** command.

The **vrf** keyword allows you to specify the notifications being sent to a specified IP address over a specific VRF. The VRF defines a VPN membership of a customer so data is stored using the VPN.

Regarding Notification Type Keywords

The *notification-type* keywords used in the **snmp-server host** command do not always match the keywords used in the corresponding **snmp-server enable traps** command. For example, the notification keyword applicable to MPLS traffic engineering tunnels is specified as **mpls-traffic-eng** (containing two dashes and no intervening spaces). The corresponding parameter in the **snmp-server enable traps** command is specified as **mpls traffic-eng** (containing an intervening space and a dash).

This syntax difference is necessary to ensure that the CLI interprets the *notification-type* keyword of the **snmp-server host** command as a unified, single-word construct, which preserves the capability of the **snmp-server host** command to accept multiple *notification-type* keywords in the CLI command line. The **snmp-server enable traps** commands, however, often use two-word constructs in order to provide hierarchical configuration options and to maintain consistency with the command syntax of related commands. Table 126 maps **snmp-server enable traps** commands to the keywords used in the **snmp-server host** command.

Table 126 Notification Keywords and Corresponding SNMP Enable Traps Commands

SNMP Enable Traps Command	SNMP Host Command Keyword
snmp-server enable traps mpls ldp	**mpls-ldp**
snmp-server enable traps mpls traffic-eng[1]	**mpls-traffic-eng**
snmp-server enable traps mpls vpn	**mpls-vpn**

1. See the *Cisco IOS Switching Services Command Reference* for documentation of this command.

Examples

If you want to configure a unique SNMP community string for traps, but you want to prevent SNMP polling access with this string, the configuration should include an access-list. In the following example, the community string is named “comaccess” and the access list is numbered 10:

```
Router(config)# snmp-server community comaccess ro 10
Router(config)# snmp-server host 172.20.2.160 comaccess
Router(config)# access-list 10 deny any
```

The following example sends RFC 1157 SNMP traps to the host specified by the name myhost.cisco.com. Other traps are enabled, but only SNMP traps are sent because only **snmp** is specified in the **snmp-server host** command. The community string is defined as comaccess.

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com comaccess snmp
```

The following example sends the SNMP and Cisco environmental monitor enterprise-specific traps to address 172.30.2.160:

```
Router(config)# snmp-server enable traps snmp
Router(config)# snmp-server enable traps envmon
Router(config)# snmp-server host 172.30.2.160 public snmp envmon
```

The following example enables the router to send all traps to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com public
```

The following example will not send traps to any host. The BGP traps are enabled for all hosts, but only the ISDN traps are enabled to be sent to a host.

```
Router(config)# snmp-server enable traps bgp
Router(config)# snmp-server host bob public isdn
```

The following example enables the router to send all inform requests to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

The following example sends HSRP MIB informs to the host specified by the name myhost.cisco.com. The community string is defined as public.

```
Router(config)# snmp-server enable traps hsrp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public hsrp
```

The following example sends all SNMP notifications to xyz.com over the VRF named trap-vrf:

```
Router(config)# snmp-server host xyz.com vrf trap-vrf
```

Related Commands

Command	Description
snmp-server enable peer-trap poor qov	Enable poor quality of voice notifications for applicable calls associated with a specific voice dial peer.
snmp-server enable traps	Enables SNMP notifications (traps and informs).
snmp-server informs	Specifies inform request options.
snmp-server link trap	Enables linkUp/linkDown SNMP traps which are compliant with RFC 2233.
snmp-server trap-source	Specifies the interface (and hence the corresponding IP address) that an SNMP trap should originate from.
snmp-server trap-timeout	Defines how often to try resending trap messages on the retransmission queue.

snmp-server informs

To specify inform request options, use the **snmp-server informs** command in global configuration mode. To return the settings to the defaults, use the **no** form of this command.

snmp-server informs [**retries** *retries*] [**timeout** *seconds*] [**pending** *pending*]

no snmp-server informs [**retries** *retries*] [**timeout** *seconds*] [**pending** *pending*]

Syntax Description

retries *retries*	(Optional) Maximum number of times to resend an inform request. The default is 3.
timeout *seconds*	(Optional) Number of seconds to wait for an acknowledgment before resending. The default is 30 seconds.
pending *pending*	(Optional) Maximum number of informs waiting for acknowledgments at any one time. When the maximum is reached, older pending informs are discarded. The default is 25.

Defaults

Inform requests are resent three times. Informs are resent after 30 seconds if no response is received. The maximum number of informs waiting for acknowledgments at any one time is 25.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Examples

The following example increases the pending queue size if you are seeing a large number of inform drops:

```
snmp-server informs pending 50
```

The following example increases the default timeout if you are sending informs over slow network links. Because informs will be sitting in the queue for a longer period of time, you may also need to increase the pending queue size.

```
snmp-server informs timeout 60 pending 40
```

The following example decreases the default timeout if you are sending informs over very fast links:

```
snmp-server informs timeout 5
```

The following example increases the retry count if you are sending informs over unreliable links. Because informs will be sitting in the queue for a longer period of time, you may need to increase the pending queue size.

```
snmp-server informs retries 10 pending 45
```

Related Commands

Command	Description
snmp-server enable traps	Enables a router to send SNMP traps and informs.

snmp-server location

To set the system location string, use the **snmp-server location** command in global configuration mode. To remove the location string, use the **no** form of this command.

snmp-server location *text*

no snmp-server location

Syntax Description

text	String that describes the system location information.

Defaults

No system location string is set.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example shows how to set a system location string:

```
snmp-server location Building 3/Room 214
```

Related Commands

Command	Description
snmp-server contact	Sets the system contact (sysContact) string.

snmp-server manager session-timeout

To set the amount of time before a nonactive session is destroyed, use the **snmp-server manager session-timeout** command in global configuration mode. To return the value to its default, use the **no** form of this command.

snmp-server manager session-timeout *seconds*

no snmp-server manager session-timeout

Syntax Description

seconds	Number of seconds before an idle session is timed out. The default is 600 seconds.

Defaults

Idle sessions time out after 600 seconds (10 minutes).

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Sessions are created when the SNMP manager in the router sends SNMP requests, such as inform requests, to a host or receives SNMP notifications from a host. One session is created for each destination host. If there is no further communication between the router and host within the session timeout period, the session will be deleted.

The router tracks statistics, such as the average round-trip time required to reach the host, for each session. Using the statistics for a session, the SNMP manager in the router can set reasonable timeout periods for future requests, such as informs, for that host. If the session is deleted, all statistics are lost. If another session with the same host is later created, the request timeout value for replies will return to the default value.

However, sessions consume memory. A reasonable session timeout value should be large enough such that regularly used sessions are not prematurely deleted, yet small enough such that irregularly used, or one-shot sessions, are purged expeditiously.

Examples

The following example sets the session timeout to a larger value than the default:

```
snmp-server manager
snmp-server manager session-timeout 1000
```

Related Commands

Command	Description
show snmp pending	Displays the current set of pending SNMP requests.
show snmp sessions	Displays the current SNMP sessions.
snmp-server manager	Starts the SNMP manager process.

snmp-server manager

To start the Simple Network Management Protocol (SNMP) manager process, use the **snmp-server manager** command in global configuration mode. To stop the SNMP manager process, use the **no** form of this command.

snmp-server manager

no snmp-server manager

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

The SNMP manager process sends SNMP requests to agents and receives SNMP responses and notifications from agents. When the SNMP manager process is enabled, the router can query other SNMP agents and process incoming SNMP traps.

Most network security policies assume that routers will be accepting SNMP requests, sending SNMP responses, and sending SNMP notifications. With the SNMP manager functionality enabled, the router may also be sending SNMP requests, receiving SNMP responses, and receiving SNMP notifications. The security policy implementation may need to be updated prior to enabling this functionality.

SNMP requests are typically sent to UDP port 161. SNMP responses are typically sent from UDP port 161. SNMP notifications are typically sent to UDP port 162.

Examples

The following example enables the SNMP manager process:

```
snmp-server manager
```

Related Commands

Command	Description
show snmp	Checks the status of SNMP communications.
show snmp pending	Displays the current set of pending SNMP requests.
show snmp sessions	Displays the current SNMP sessions.
snmp-server manager session-timeout	Sets the amount of time before a nonactive session is destroyed.

snmp-server packetsize

To establish control over the largest Simple Network Management Protocol (SNMP) packet size permitted when the SNMP server is receiving a request or generating a reply, use the **snmp-server packetsize** command in global configuration mode. To restore the default value, use the **no** form of this command.

snmp-server packetsize *byte-count*

no snmp-server packetsize

Syntax Description

byte-count	Integer byte count from 484 to 8192. The default is 1500 bytes.

Defaults

1500 bytes

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example establishes a packet filtering of a maximum size of 1024 bytes:

```
snmp-server packetsize 1024
```

Related Commands

Command	Description
snmp-server queue-length	Establishes the message queue length for each trap host.

snmp-server queue-length

To establish the message queue length for each trap host, use the **snmp-server queue-length** command in global configuration mode.

snmp-server queue-length *length*

Syntax Description

length	Integer that specifies the number of trap events that can be held before the queue must be emptied.

Defaults

10 events

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command defines the length of the message queue for each trap host. Once a trap message is successfully transmitted, software will continue to empty the queue, but never faster than at a rate of four trap messages per second.

During device bootup, there is a possibility that some traps could be dropped because of trap queue overflow on the device. If you suspect this is occurring, you can increase the size of the trap queue (for example, to 100) to determine if traps are then able to be sent during bootup.

Examples

In the following example, the SNMP notification queue is increased to 50 events:

```
Router(config)# snmp-server queue-length 50
```

Related Commands

Command	Description
snmp-server packetsize	Establishes control over the largest SNMP packet size permitted when the SNMP server is receiving a request or generating a reply.

snmp-server system-shutdown

To use the Simple Network Management Protocol (SNMP) message reload feature, the router configuration must include the **snmp-server system-shutdown** command in global configuration mode. To prevent an SNMP system-shutdown request (from an SNMP manager) from resetting the Cisco agent, use the **no** form of this command.

snmp-server system-shutdown

no snmp-server system-shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

This command is not included in the configuration file.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example enables the SNMP message reload feature:

```
snmp-server system-shutdown
```

snmp-server tftp-server-list

To limit the TFTP servers used via Simple Network Management Protocol (SNMP) controlled TFTP operations (saving and loading configuration files) to the servers specified in an access list, use the **snmp-server tftp-server-list** command in global configuration mode. To disable this function, use the **no** form of this command.

snmp-server tftp-server-list *number*

no snmp-server tftp-server-list

Syntax Description

number	Standard IP access list number from 1 to 99.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.2	This command was introduced.

Examples

The following example limits the TFTP servers that can be used for configuration file copies via SNMP to the servers in access list 44:

```
snmp-server tftp-server-list 44
```

snmp-server trap link

To enable linkUp/linkDown Simple Network Management Protocol (SNMP) traps that are compliant with RFC2233, use the **snmp-server trap link** command in global configuration mode. To disable IETF-compliant functionality and revert to the default Cisco implementation of linkUp/linkDown traps, use the **no** form of this command.

snmp-server trap link ietf

no snmp-server trap link ietf

Syntax Description

ietf	This required keyword indicates to the command parser that you would like to link functionality of SNMP linkUp/linkDown traps to the Internet Engineering Task Force (IETF) standard (as opposed to the previous Cisco implementation).

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

The **snmp-server trap link ietf** command is used to configure your router to use the RFC2233 IETF standards-based implementation of linkUp/linkDown traps. This command is disabled by default to allow you to continue using the earlier Cisco implementation of linkUp/linkDown traps if you so choose.

However, please note that when using the default Cisco object definitions, linkUp/linkDown traps are not generated correctly for sub-interfaces. In the default implementation an arbitrary value is used for the *locIfReason* object in linkUp/linkDown traps for sub-interfaces, which may give you unintended results. This is because the *locIfReason* object is not defined for sub-interfaces in the current Cisco implementation, which uses OLD-CISCO-INTERFACES-MIB.my.

If you do not enable this functionality, the link trap varbind list will consist of {ifIndex, ifDescr, ifType, locIfReason}. After you enable this functionality with the **snmp-server trap link ietf** command, the varbind list will consist of {inIndex, ifAdminStatus,ifOperStatus, if Descr, ifType}. The *locIfReason* object will also be conditionally included in this list depending on whether meaningful information can be retrieved for that object. A configured sub-interface will generate retrievable information. On non-HWIDB interfaces, there will be no defined value for *locIfReason*, so it will be omitted from the trap message.

Examples

The following example shows the enabling of the RFC 2233 linkUp/linkDown traps, starting in privileged EXEC mode:

```
Router# config term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# snmp-server trap link ietf
Router(config)# end
Router# more system:running config
.
.
.
!
snmp-server engineID local 00000009000000A1616C2056
snmp-server community public RO
snmp-server community private RW
snmp-server trap link ietf
!
.
.
.
```

Related Commands

Command	Description
debug snmp packets	Displays information about every SNMP packet sent or received by the router for the purposes of troubleshooting.

snmp-server trap-authentication

The **snmp-server trap-authentication** command has been replaced by the **snmp-server enable traps snmp authentication** command. See the description of the **snmp-server enable traps snmp** command in this chapter for more information.

snmp-server trap-source

To specify the interface (and hence the corresponding IP address) that a Simple Network Management Protocol (SNMP) trap should originate from, use the **snmp-server trap-source** command in global configuration mode. To remove the source designation, use the **no** form of the command.

snmp-server trap-source *interface*

no snmp-server trap-source

Syntax Description

interface	Interface from which the SNMP trap originates. The argument includes the interface type and number in platform-specific syntax (for example, *type*/*slot*/*port*).

Defaults

No interface is specified.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When an SNMP trap or inform is sent from a Cisco SNMP server, it has a notification address of whatever interface it happened to go out of at that time. Use this command to monitor notifications from a particular interface.

Examples

The following example specifies that the IP address for Ethernet interface 0 is the source for all SNMP notifications:

```
Router(config)# snmp-server trap-source ethernet 0
```

The following example specifies that the IP address for the Ethernet interface in slot2, port 1 is the source for all SNMP notifications:

```
Router(config)# snmp-server trap-source ethernet 2/1
```

Related Commands

Command	Description
snmp-server enable traps	Enables a router to send SNMP traps and informs.
snmp-server host	Specifies the recipient of an SNMP notification operation.

snmp-server trap-timeout

To define how often to try resending trap messages on the retransmission queue, use the **snmp-server trap-timeout** command in global configuration mode.

snmp-server trap-timeout *seconds*

Syntax Description

seconds	Integer that sets the interval (in seconds) for resending the messages. The default is 30 seconds.

Defaults

30 seconds

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Before the Cisco IOS software tries to send a trap, it looks for a route to the destination address. If there is no known route, the trap is saved in a retransmission queue. The **snmp server trap-timeout** command determines the number of seconds between retransmission attempts.

Examples

The following example sets an interval of 20 seconds to try resending trap messages on the retransmission queue:

```
snmp-server trap-timeout 20
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server queue-length	Establishes the message queue length for each trap host.

snmp-server user

To configure a new user to a Simple Network Management Protocol (SNMP) group, use the **snmp-server user** command in global configuration mode. To remove a user from an SNMP group, use the **no** form of the command.

snmp-server user *username group-name* [**remote** *host* [**udp-port** *port*]]
{**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** *access-list*]

no snmp-server user

Syntax Description

username	The name of the user on the host that connects to the agent.
group-name	The name of the group to which the user belongs.
remote *host*	(Optional) Specifies a remote SNMP entity to which the user belongs, and the hostname or IP address of that entity.
udp-port *port*	(Optional) Specifies the UDP port number of the remote host. The default is UDP port 162.
v1	Specifies that SNMPv1 should be used.
v2c	Specifies that SNMPv2c should be used.
v3	Specifies that the SNMPv3 security model should be used. Allows the use of the **encrypted** and/or **auth** keywords.
encrypted	(Optional) Specifies whether the password appears in encrypted format (a series of digits, masking the true characters of the string).
auth	(Optional) Specifies which authentication level should be used.
md5	The HMAC-MD5-96 authentication level.
sha	The HMAC-SHA-96 authentication level.
auth-password	A string (not to exceed 64 characters) that enables the agent to receive packets from the host.
access *access-list*	(Optional) Specifies an access list to be associated with this SNMP user. The *access-list* argument represents a value from1 to 99 that is the identifier of the standard IP access list.

Defaults

Table 127 describes default behaviors for encryption, passwords and access lists.

Table 127 snmp-server user Default Descriptions

Characteristic	Default
encryption	Not present by default. The **encrypted** keyword is used to specify that the **auth** and **priv** passwords are **MD5** digests and not text passwords.
passwords	Assumed to be text strings.
access lists	Access from all IP access lists is permitted.
remote users	All users are assumed to be local to this SNMP engine unless you specify they are remote with the **remote** keyword.

Command Modes Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines To configure a remote user, specify the IP address or port number for the remote SNMP agent of the device where the user resides. Also, before you configure remote users for a particular agent, configure the SNMP engine ID, using the command **snmp-server engineID** with the **remote** option. The remote agent's SNMP engine ID is needed when computing the authentication/privacy digests from the password. If the remote engine ID is not configured first, the configuration command will fail.

SNMP passwords are localized using the SNMP engine ID of the authoritative SNMP engine. For informs, the authoritative SNMP agent is the remote agent. You need to configure the remote agent's SNMP engine ID in the SNMP database before you can send proxy requests or informs to it.

Related Commands

Command	Description
show snmp user	Displays information on each SNMP username in the group username table.

snmp-server view

To create or update a view entry, use the **snmp-server view** command in global configuration mode. To remove the specified Simple Network Management Protocol (SNMP) server view entry, use the **no** form of this command.

snmp-server view *view-name oid-tree* {**included** | **excluded**}

no snmp-server view *view-name*

Syntax Description

view-name	Label for the view record that you are updating or creating. The name is used to reference the record.
oid-tree	Object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as system. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4.
included | **excluded**	Type of view. You must specify either **included** or **excluded**.

Defaults

No view entry exists.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Other SNMP commands require a view as an argument. You use this command to create a view to be used as arguments for other commands that create records including a view.

Two standard predefined views can be used when a view is required, instead of defining a view. One is *everything*, which indicates that the user can see all objects. The other is *restricted*, which indicates that the user can see three groups: system, snmpStats, and snmpParties. The predefined views are described in RFC 1447.

The first **snmp-server** command that you enter enables both versions of SNMP.

Examples

The following example creates a view that includes all objects in the MIB-II subtree:

```
snmp-server view mib2 mib-2 included
```

The following example creates a view that includes all objects in the MIB-II system group and all objects in the Cisco enterprise MIB:

```
snmp-server view phred system included
snmp-server view phred cisco included
```

The following example creates a view that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group:

```
snmp-server view agon system included
snmp-server view agon system.7 excluded
snmp-server view agon ifEntry.*.1 included
```

Related Commands

Command	Description
snmp-server community	Sets up the community access string to permit access to the SNMP protocol.

sntp broadcast client

To use the Simple Network Time Protocol (SNTP) to accept Network Time Protocol (NTP) traffic from any broadcast server, use the **sntp broadcast client** command in global configuration mode to configure a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router. To prevent the router from accepting broadcast traffic, use the **no** form of this command.

sntp broadcast client

no sntp broadcast client

Syntax Description

This command has no arguments or keywords.

Defaults

The router does not accept SNTP traffic from broadcast servers.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

SNTP is a compact, client-only version of the NTP. SNMP can only receive the time from NTP servers; it cannot be used to provide time services to other systems.

SNTP typically provides time within 100 milliseconds of the accurate time, but it does not provide the complex filtering and statistical mechanisms of NTP. In addition, SNTP does not authenticate traffic, although you can configure extended access lists to provide some protection.

You must configure the router with either this command or the **sntp server** global configuration command to enable SNTP.

Examples

The following example enables the router to accept broadcast NTP packets and shows sample **show sntp** command output:

```
Router(config)# sntp broadcast client
Router(config)# end
Router#
%SYS-5-CONFIG: Configured from console by console
Router# show sntp

SNTP server     Stratum   Version    Last Receive
172.21.28.34       4         3        00:00:36    Synced  Bcast

Broadcast client mode is enabled.
```

Related Commands

Command	Description
show sntp	Displays information about SNTP on a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router.
sntp server	Configures a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use SNTP to request and accept NTP traffic from a time server.

sntp server

To configure a Cisco 800, Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use the Simple Network Time Protocol (SNTP) to request and accept Network Time Protocol (NTP) traffic from a stratum 1 time server, use the **sntp server** command in global configuration mode. To remove a server from the list of NTP servers, use the **no** form of this command.

sntp server {*address* | *hostname*} [**version** *number*]

no sntp server {*address* | *hostname*}

Syntax Description

address	IP address of the time server.
hostname	Host name of the time server.
version *number*	(Optional) Version of NTP to use. The default is 1.

Defaults

The router does not accept SNTP traffic from a time server.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

SNTP is a compact, client-only version of the NTP. SNMP can only receive the time from NTP servers; it cannot be used to provide time services to other systems.

SNTP typically provides time within 100 milliseconds of the accurate time, but it does not provide the complex filtering and statistical mechanisms of NTP. In addition, SNTP does not authenticate traffic, although you can configure extended access lists to provide some protection.

Enter this command once for each NTP server.

You must configure the router with either this command or the **sntp broadcast client** global configuration command in order to enable SNTP.

SNTP time servers should operate only at the root (stratum 1) of the subnet, and then only in configurations where no other source of synchronization other than a reliable radio or modem time service is available. A stratum 2 server cannot be used as an SNTP time server. The use of SNTP rather than NTP in primary servers should be carefully considered.

Examples

The following example enables the router to request and accept NTP packets from the server at 172.21.118.9 and displays sample **show sntp** command output:

```
Router(config)# sntp server 172.21.118.9
Router(config)# end
Router#
%SYS-5-CONFIG: Configured from console by console
```

```
Router# show sntp

SNTP server     Stratum   Version    Last Receive
172.21.118.9       5         3        00:01:02    Synced
```

Related Commands

Command	Description
show sntp	Displays information about SNTP on a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router.
sntp broadcast client	Configures a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use SNTP to accept NTP traffic from any broadcast server.

special-character-bits

To configure the number of data bits per character for special characters such as software flow control characters and escape characters, use the **special-character-bits** command in line configuration mode. To restore the default value, use the **no** form of this command.

special-character-bits {**7** | **8**}

no special-character-bits

Syntax Description

7	Selects the 7-bit ASCII character set. This is the default.
8	Selects the full 8-bit character set for special characters.

Defaults

7-bit ASCII character set

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Setting the special character bits to 8 allows you to use twice as many special characters as with the 7-bit ASCII character set. The special characters affected by this setting are the escape, hold, stop, start, disconnect, and activation characters.

Examples

The following example allows the full 8-bit international character set for special characters on line 5:

```
Router(config)# line 5
Router(config-line)# special-character-bits 8
```

Related Commands

Command	Description
default-value exec-character-bits	Defines the EXEC character width for either 7 bits or 8 bits.
default-value special-character-bits	Configures the flow control default value from a 7-bit width to an 8-bit width.
exec-character-bits	Configures the character widths of EXEC and configuration command characters.
terminal exec-character-bits	Locally changes the ASCII character set used in EXEC and configuration command characters for the current session.
terminal special-character-bits	Changes the ASCII character widths to accept special characters for the current terminal line and session.

squeeze

To permanently erase files tagged as "deleted" or "error" on Class A Flash file systems, use the **squeeze** command in EXEC mode.

squeeze [**/nolog**] [**/quiet**] *filesystem***:**

Syntax Description

/nolog	(Optional) Disables the squeeze log (recovery data) and accelerates the squeeze process.
/quiet	(Optional) Disables status messages during the squeeze process.
*filesystem***:**	The Flash file system, followed by a colon.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(1)	This command was implemented on the Cisco 2600 and Cisco 3600 series routers.
12.2(4)XL	This command was implemented on the Cisco 1700 series routers.
12.1(9), 12.0(17)S 12.0(17)ST, 12.2(2), 12.2(2)T, 12.2(2)B, 12.1(9)E	The **/nolog** and **/quiet** keywords were added.

Usage Guidelines

When Flash memory is full, you might need to rearrange the files so that the space used by the files marked "deleted" can be reclaimed. (This "squeeze" process is required for linear Flash memory cards to make sectors contiguous; the free memory must be in a "block" to be usable.)

When you enter the **squeeze** command, the router copies all valid files to the beginning of Flash memory and erases all files marked "deleted." After the squeeze process is completed, you can write to the reclaimed Flash memory space.

Caution After performing the squeeze process you cannot recover deleted files using the **undelete** EXEC mode command.

In addition to removing deleted files, the **squeeze** command removes any files that the system has marked as "error". An error file is created when a file write fails (for example, the device is full). To remove error files, you must use the **squeeze** command.

Rewriting Flash memory space during the squeeze operation may take several minutes.

Using the **/nolog** keyword disables the log for the squeeze process. In most cases this will speed up the squeeze process. However, if power is lost or the Flash card is removed during the squeeze process, all the data on the Flash card will be lost, and the device will have to be reformatted.

Note Using the **/nolog** keyword makes the squeeze process uninterruptible.

Using the **/quiet** keyword disables the output of status messages to the console during the squeeze process.

If the optional keywords are not used, the progress of squeeze process will be displayed to the console, a log for the process will be maintained, and the squeeze process is interruptible.

On Cisco 2600 or Cisco 3600 series routers, the entire file system needs to be erased once before the **squeeze** command can be used. After being erased once, the **squeeze** command should operate properly on the Flash file system for the rest of the Flash file system's history.

To erase an entire flash file system on a Cisco 2600 or 3600 series router, perform the following steps:

Step 1 If the Flash file system has multiple partitions, enter the **no partition** command to remove the partitions. The reason for removing partitions is to ensure that the entire Flash file system is erased. The **squeeze** command can be used in a Flash file system with partitions after the Flash file system is erased once.

Step 2 Enter the **erase** command to erase the Flash file system.

Examples

In the following example, the file named config1 is deleted, and then the **squeeze** command is used to reclaim the space used by that file. The **/nolog** option is used to speed up the squeeze process.

```
Router# delete config1
Delete filename [config1]?
Delete slot0:conf? [confirm]
Router# dir slot0:
! Note that the deleted file name appears in square brackets
Directory of slot0:/

    1  -rw-     4300244   Apr 02 2001 03:18:07  c7200-boot-mz.122-0.14
    2  -rw-        2199   Apr 02 2001 04:45:15  [config1]
    3  -rw-     4300244   Apr 02 2001 04:45:23  image
20578304 bytes total (11975232 bytes free)
!20,578,304 - 4,300,244 - 4,300,244 - 2,199 - 385 = 11975232


Router# squeeze /nolog slot0:
%Warning: Using /nolog option would render squeeze operation uninterruptible.
All deleted files will be removed. Continue? [confirm]
Squeeze operation may take a while. Continue? [confirm]

Squeeze of slot0 completed in 291.832 secs .
Router# dir slot0:
Directory of slot0:/

    1  -rw-     4300244   Apr 02 2001 03:18:07  c7200-boot-mz.122-0.14
    2  -rw-     4300244   Apr 02 2001 04:45:23  image

20578304 bytes total (11977560 bytes free)
!20,578,304 - 4,300,244 - 4,300,244 - 256 = 11977560
```

Related Commands

Command	Description
delete	Deletes a file on a Flash memory device.
dir	Displays a list of files on a file system.
undelete	Recovers a file marked “deleted” on a Class A or Class B Flash file system.

state-machine

To specify the transition criteria for the state of a particular state machine, use the **state-machine** command in global configuration mode. To remove a particular state machine from the configuration, use the **no** form of this command.

state-machine *name state first-character last-character* [*next-state* | **transmit**]

no state-machine *name*

Syntax Description

name	Name for the state machine (used in the **dispatch-machine** line configuration command). The user can specify any number of state machines, but each line can have only one state machine associated with it.
state	State being modified. There are a maximum of eight states per state machine. Lines are initialized to state 0 and return to state 0 after a packet is transmitted.
first-character last-character	Specifies a range of characters. Use ASCII numerical values. If the state machine is in the indicated state, and the next character input is within this range, the process goes to the specified next state. Full 8-bit character comparisons are done, so the maximum value is 255. Ensure that the line is configured to strip parity bits (or not generate them), or duplicate the low characters in the upper half of the space.
next-state	(Optional) State to enter if the character is in the specified range.
transmit	(Optional) Causes the packet to be transmitted and the state machine to be reset to state 0. Recurring characters that have not been explicitly defined to have a particular action return the state machine to state 0.

Defaults

No transition criteria are specified.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command is paired with the **dispatch-machine** line configuration command, which defines the line on which the state machine is effective.

Examples

In the following example a dispatch machine named "*function*" is configured to ensure that the function key characters on an ANSI terminal are kept in one packet. Because the default in the example is to remain in state 0 without sending anything, normal key signals are sent immediately.

```
Router(config)# line 1 20
Router(config-line)# dispatch-machine function
Router(config-line)# exit
Router(config)# state-machine function 0 0 255 transmit
```

Related Commands

Command	Description
dispatch-character	Defines a character that causes a packet to be sent.
dispatch-machine	Specifies an identifier for a TCP packet dispatch state machine on a particular line.
dispatch-timeout	Sets the character dispatch timer.

statistics-distribution-interval

To set the time interval for each statistics distribution kept for the Service Assurance Agent (SAA), use the **statistics-distribution-interval** command in SAA RTR configuration mode. To return to the default value, use the **no** form of this command.

statistics-distribution-interval *milliseconds*

no statistics-distribution-interval

Syntax Description

milliseconds	Number of milliseconds (ms) used for each statistics distribution kept. The default is 20 ms.

Defaults

20 ms

Command Modes

SAA RTR configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

In most situations, you do not need to change the statistical distribution interval or size. Only change the interval or size when distributions are needed, for example, when performing statistical modeling of your network. To set the statistical distributions size, use the **distributions-of-statistics-kept** SAA RTR configuration command.

Examples

In the following example, the distribution is set to five and the distribution interval is set to 10 ms. This means that the first distribution will contain statistics from 0 to 9 ms, the second distribution will contain statistics from 10 to 19 ms, the third distribution will contain statistics from 20 to 29 ms, the fourth distribution will contain statistics from 30 to 39 ms, and the fifth distribution will contain statistics from 40 ms to infinity.

```
Router(config)# rtr 1
Router(config-rtr)# type echo protocol ipIcmpEcho 172.28.161.21
Router(config-rtr)# distribution-of-statistics-kept 5
Router(config-rtr)# statistics-distribution-interval 10
```

Related Commands

Command	Description
distributions-of-statistics-kept	Sets the number of statistic distributions kept per hop during the SAA operation's lifetime.
hops-of-statistics-kept	Set the number of hops for which statistics are maintained per path for the SAA operation.

Command	Description
hours-of-statistics-kept	Sets the number of hours for which statistics are maintained for the SAA operation.
paths-of-statistics-kept	Sets the number of paths for which statistics are maintained per hour for the SAA operation.
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.

stopbits

To set the number of the stop bits transmitted per byte, use the **stopbits** command in line configuration mode. To restore the default value, use the **no** form of this command.

stopbits {**1** | **1.5** | **2**}

no stopbits

Syntax Description

1	One stop bit.
1.5	One and one-half stop bits.
2	Two stop bits.This is the default.

Defaults

2 stop bits per byte

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Communication protocols provided by devices such as terminals and modems often require a specific stop-bit setting.

Examples

In the following example, the stop bits transmitted per byte are changed from the default of two stop bits to one stop bit as a performance enhancement for line 4:

```
Router(config)# line 4
Router(config-line)# stopbits 1
```

Related Commands

Command	Description
terminal stopbits	Changes the number of stop bits sent per byte by the current terminal line during an active session.

tag

To create a user-specified identifier for an Service Assurance Agent (SAA) operation, use the **tag** command in SAA RTR configuration mode. To remove a tag from an operation, use the **no** form of this command.

tag *text*

no tag

Syntax Description

text	Name of a group that this operation belongs to. From 0 to 16 ASCII characters.

Defaults

No operations are tagged.

Command Modes

SAA RTR configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

An operation tag is normally used to logically link operations in a group

Tags can be used to support automation (for example, by using the same tag for two different operations on two different routers echoing the same target).

Examples

In the following example, operation 1 is tagged with the label bluebell:

```
Router(config)# rtr 1
Router(config-rtr)# type echo protocol ipIcmpEcho 172.16.1.176
Router(config-rtr)# tag bluebell
```

Related Commands

Command	Description
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.

template (cns)

To specify a list of Cisco Networking Services (CNS) connect templates within a CNS connect profile to be applied to a router's configuration, use the **template** command in CNS connect configuration mode. To disable this CNS connect template, use the **no** form of this command.

template *name* [*...name*]

no template *name* [*...name*]

Syntax Description

name	Name of the CNS connect template to be applied to a router's configuration. The ellipsis (...) in the command syntax indicates that the command input can include multiple *name* arguments. Multiple *name* arguments are delimited by a single space.

Defaults

No CNS connect templates are specified.

Command Modes

CNS connect configuration

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.3(9)	This command was integrated into Cisco IOS Release 12.3(9).

Usage Guidelines

First use the **cns connect** command to enter CNS connect configuration mode and define the parameters of a CNS connect profile for connecting to the CNS configuration engine. Then use the following CNS connect commands to create a CNS connect profile:

- **discover**
- **template**

A CNS connect profile specifies the **discover** commands and associated **template** commands that are to be applied to a router's configuration. The **template** command specifies the list of CNS connect templates that is to be applied to a router's configuration. The templates in the list are applied one at a time. That is, when the **template** command is processed, the first template in the list is applied to the router's configuration. The router then tries to ping the CNS configuration engine. If the ping fails, then the first template in the list is removed from the router's configuration and the second template in the list is applied and so on.

The configuration mode in which the CNS connect templates are applied is specified by the immediately preceding **discover** command. (If there are no preceding **discover** commands, the templates are applied in global configuration mode.) When multiple **discover** and **template** commands are configured in a CNS connect profile, they are processed in the order in which they are entered.

Examples

The following example shows how to create a CNS connect profile named profile-1:

```
Router (config)# cns connect profile-1
Router (config-cns-conn)# discover interface Serial
Router (config-cns-conn)# template temp-A1 temp-A2
Router (config-cns-conn)# template temp-B1 temp-B2
Router (config-cns-conn)# exit
Router (config)#
```

In this example, the following sequence of events occur for all serial interfaces when the **cns connect profile-1** command is processed. Assume all ping attempts to the CNS configuration engine are unsuccessful.

1. Enter interface configuration mode and apply all commands in the temp-A1 template to the router's configuration.
2. Enter interface configuration mode and apply all commands in the temp-B1 template to the router's configuration.
3. Try to ping the CNS configuration engine.
4. Enter interface configuration mode and remove all commands in the temp-B1 template from the router's configuration.
5. Enter interface configuration mode and apply all commands in the temp-B2 template to the router's configuration.
6. Try to ping the CNS configuration engine.
7. Enter interface configuration mode and remove all commands in the temp-B2 template from the router's configuration.
8. Enter interface configuration mode and remove all commands in the temp-A1 template from the router's configuration.
9. Enter interface configuration mode and apply all commands in the temp-A2 template to the router's configuration.
10. Enter interface configuration mode and apply all commands in the temp-B1 template to the router's configuration.
11. Try to ping the CNS configuration engine.
12. Enter interface configuration mode and remove all commands in the temp-B1 template from the router's configuration.
13. Enter interface configuration mode and apply all commands in the temp-B2 template to the router's configuration.
14. Try to ping the CNS configuration engine.
15. Enter interface configuration mode and remove all commands in the temp-B2 template from the router's configuration.
16. Enter interface configuration mode and remove all commands in the temp-A2 template from the router's configuration.

Related Commands

Command	Description
cli (cns)	Specifies the command lines of a CNS connect template.
cns connect	Enters CNS connect configuration mode and defines the parameters of a CNS connect profile for connecting to the CNS configuration engine.

Command	Description
cns template connect	Enters CNS template connect configuration mode and defines the name of a CNS connect template.
discover (cns)	Defines the interface parameters within a CNS connect profile for connecting to the CNS configuration engine.

terminal databits

To change the number of data bits per character for the current terminal line for this session, use the **terminal databits** command in EXEC mode.

terminal databits {**5** | **6** | **7** | **8**}

Syntax Description

5	Five data bits per character.
6	Six data bits per character.
7	Seven data bits per character.
8	Eight data bits per character. This is the default.

Defaults

8 data bits per character

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Communication protocols provided by devices such as terminals and modems often require a specific data bit setting. The **terminal databits** command can be used to mask the high bit on input from devices that generate 7 data bits with parity. If parity is being generated, specify 7 data bits per character. If no parity generation is in effect, specify 8 data bits per character. The other keywords (**5** and **6**) are supplied for compatibility with older devices and are generally not used.

Examples

In the following example, the databits per character is changed to seven for the current session:

```
Router# terminal databits 7
```

Related Commands

Command	Description
databits	Sets the number of data bits per character that are interpreted and generated by the router hardware.
terminal parity	Defines the generation of the parity bit for the current terminal line and session.

terminal data-character-bits

To set the number of data bits per character that are interpreted and generated by the Cisco IOS software for the current line and session, use the **terminal data-character-bits** command in EXEC mode.

terminal data-character-bits {**7** | **8**}

Syntax Description

7	Seven data bits per character.
8	Eight data bits. This is the default.

Defaults

8 data bits per character

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command is used primarily to strip parity from X.25 connections on routers with the protocol translation software option. The **terminal data-character-bits** command does not work on hard-wired lines.

Examples

The following example sets the data bits per character to seven on the current line:

```
Router# terminal data-character-bits 7
```

Related Commands

Command	Description
data-character-bits	Sets the number of data bits per character that are interpreted and generated by the Cisco IOS software.

terminal dispatch-character

To define a character that causes a packet to be sent for the current session, use the **terminal dispatch-character** command in EXEC mode.

terminal dispatch-character *ascii-number* [*ascii-number2 . . . ascii-number*]

Syntax Description

ascii-number	The ASCII decimal representation of the character, such as Return (ASCII character 13) for line-at-a-time transmissions.
ascii-number2 . . . ascii-number	(Optional) Additional decimal representations of characters. This syntax indicates that you can define any number of characters as dispatch characters.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

At times, you might want to queue up a string of characters until they fill a complete packet and then transmit the packet to a remote host. This can make more efficient use of a line, because the access server or router normally dispatches each character as it is entered.

Examples

The following example defines the characters Ctrl-D (ASCII decimal character 4) and Ctrl-Y (ASCII decimal character 25) as the dispatch characters:

```
Router# terminal dispatch-character 4 25
```

Related Commands

Command	Description
dispatch-character	Defines a character that causes a packet to be sent.

terminal dispatch-timeout

To set the character dispatch timer for the current terminal line for the current session, use the **terminal dispatch-timeout** command in EXEC mode.

terminal dispatch-timeout *milliseconds*

Syntax Description

milliseconds	Integer that specifies the number of milliseconds that the router waits after it puts the first character into a packet buffer before sending the packet. During this interval, more characters can be added to the packet, which increases the processing efficiency of the remote host.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command to increase the processing efficiency of the remote host.

The **dispatch-timeout** line configuration command causes the software to buffer characters into packets for transmission to the remote host. The Cisco IOS software sends a packet a specified amount of time after the first character is put into the buffer. You can use the **terminal dispatch-timeout** and **terminal dispatch-character** line configuration commands together. In this case, the software dispatches a packet each time the dispatch character is entered, or after the specified dispatch timeout interval, depending on which condition is met first.

Note The router response time might appear intermittent if the timeout interval is greater than 100 milliseconds and remote echoing is used.

Examples

In the following example, the dispatch timeout timer is set to 80 milliseconds:

```
Router# terminal dispatch-timeout 80
```

Related Commands

Command	Description
dispatch-timeout	Sets the character dispatch timer for a specified line or group of lines.

terminal download

To temporarily set the ability of a line to act as a transparent pipe for file transfers for the current session, use the **terminal download** command in EXEC mode.

terminal download

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You can use this feature to run a program such as KERMIT, XMODEM, or CrossTalk that downloads a file across an access server or router line. This command configures the terminal line to send data and is equivalent to entering all the following commands:

- **terminal telnet transparent**
- **terminal no escape-character** (see **terminal escape-character**)
- **terminal no hold-character** (see **terminal hold-character**)
- **terminal no padding 0** (see **terminal padding**)
- **terminal no padding 128** (see **terminal padding**)
- **terminal parity none**
- **terminal databits 8**

Examples

The following example configures a line to act as a transparent pipe:

```
Router# terminal download
```

terminal editing

To reenable the enhanced editing mode for only the current terminal session, use the **terminal editing** command in EXEC mode. To disable the enhanced editing mode on the current line, use the **no** form of this command.

terminal editing

terminal no editing

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command is identical to the **editing** EXEC mode command, except that it controls (enables or disables) enhanced editing for only the terminal session you are using. For a description of the available editing keys, see the description of the **editing** command in this document.

Examples

In the following example, enhanced editing mode is reenabled for only the current terminal session:

```
Router> terminal editing
```

Related Commands

Command	Description
editing	Controls CLI enhanced editing features for a particular line.

terminal escape-character

To set the escape character for the current terminal line for the current session, use the **terminal escape-character** command in EXEC mode.

terminal escape-character *ascii-number*

Syntax Description

ascii-number	ASCII decimal representation of the escape character or control sequence (for example, Ctrl-P).

Defaults

Ctrl-^ (Ctrl-Shift-6)

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

See the "ASCII Character Set and Hexidecimal Values" appendix for a list of ASCII characters and their numerical representation.

This command is useful, for example, if you have the default escape character defined for a different purpose in your keyboard file. Entering the escape character followed by the X key returns you to EXEC mode when you are connected to another computer.

Note The Break key generally cannot be used as an escape character on the console terminal because the operating software interprets the Break command on a console line as an instruction to halt the system.

Examples

In the following example, the escape character to Ctrl-P (ASCII decimal character 16) for the current session:

```
Router# terminal escape-character 16
```

Related Commands

Command	Description
escape-character	Defines a system escape character.

terminal exec-character-bits

To locally change the ASCII character set used in EXEC and configuration command characters for the current session, use the **terminal exec-character-bits** command in EXEC mode.

terminal exec-character-bits {**7** | **8**}

Syntax Description

7	Selects the 7-bit ASCII character set. This is the default.
8	Selects the full 8-bit character set.

Defaults

7-bit ASCII character set (unless set otherwise in global configuration mode)

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This EXEC command overrides the **default-value exec-character-bits** global configuration command. Configuring the EXEC character width to 8 bits enables you to view special graphical and international characters in banners, prompts, and so on.

When the user exits the session, the character width is reset to the default value established by the **exec-character-bits** global configuration command. However, setting the EXEC character width to 8 bits can also cause failures. For example, if a user on a terminal that is sending parity enters the **help** command, an "unrecognized command" message appears because the system is reading all 8 bits, and the eighth bit is not needed for the **help** command.

Examples

The following example temporarily configures the system to use a full 8-bit user interface for system banners and prompts, allowing the use of additional graphical and international characters:

```
Router# terminal exec-character-bits 8
```

Related Commands

Command	Description
exec-character-bits	Configures the character widths of EXEC and configuration command characters.

terminal flowcontrol

To set flow control for the current terminal line for the current session, use the **terminal flowcontrol** command in EXEC mode.

terminal flowcontrol {**none** | **software** [**in** | **out**] | **hardware**}

Syntax Description

none	Prevents flow control.
software	Sets software flow control.
in | **out**	(Optional) Specifies the direction of flow control: **in** causes the router to listen to flow control from the attached device, and **out** causes the router to send flow control information to the attached device. If you do not specify a direction, both directions are assumed.
hardware	Sets hardware flow control. For information about setting up the EIA/TIA-232 line, see the manual that was shipped with your product.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Flow control enables you to regulate the rate at which data can be transmitted from one point so that it is equal to the rate at which it can be received at another point. Flow control protects against loss of data because the terminal is not capable of receiving data at the rate it is being sent. You can set up data flow control for the current terminal line in one of two ways: software flow control, which you do with control key sequences, and hardware flow control, which you do at the device level.

For software flow control, the default stop and start characters are Ctrl-S and Ctrl-Q (XOFF and XON). You can change them with the **terminal stop-character** and **terminal start-character** EXEC commands.

Examples

In the following example, incoming software flow control is set for the current session:

```
Router# terminal flowcontrol software in
```

Related Commands

Command	Description
flowcontrol	Sets the method of data flow control between the terminal or other serial device and the router.

terminal full-help

To get help for the full set of user-level commands, use the **terminal full-help** command in EXEC mode.

terminal full-help

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **terminal full-help** command enables a user to see all of the help messages available from the terminal. It is used with the **show ?** command.

Examples

In the following example, the difference between the output of the **show ?** command before and after using the **terminal full-help** command is shown:

```
Router> show ?

  bootflash  Boot Flash information
  calendar   Display the hardware calendar
  clock      Display the system clock
  context    Show context information
  dialer     Dialer parameters and statistics
  history    Display the session command history
  hosts      IP domain-name, lookup style, nameservers, and host table
  isdn       ISDN information
  kerberos   Show Kerberos Values
  modemcap   Show Modem Capabilities database
  ppp        PPP parameters and statistics
  rmon       rmon statistics
  sessions   Information about Telnet connections
  snmp       snmp statistics
  terminal   Display terminal configuration parameters
  users      Display information about terminal lines
  version    System hardware and software status


Router> terminal full-help
Router> show ?

  access-expression  List access expression
  access-lists       List access lists
  aliases            Display alias commands
  apollo             Apollo network information
```

```
appletalk          AppleTalk information
arp                ARP table
async              Information on terminal lines used as router interfaces
bootflash          Boot Flash information
bridge             Bridge Forwarding/Filtering Database [verbose]
bsc                BSC interface information
bstun              BSTUN interface information
buffers            Buffer pool statistics
calendar           Display the hardware calendar
cdp                CDP information
clns               CLNS network information
clock              Display the system clock
cls                DLC user information
cmns               Connection-Mode networking services (CMNS) information
compress           Show compression statistics.
.
.
.
x25                X.25 information
xns                XNS information
xremote            XRemote statistics
```

Related Commands

Command	Description
full-help	Gets help for the full set of user-level commands.
help	Displays a brief description of the help system.

terminal history

To enable the command history function with 10 lines for the current terminal session, use the **terminal history** command in user EXEC or privileged EXEC mode. To disable the command history function, use the **no** form of this command.

terminal history

terminal no history

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled, history buffer of 10 lines

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The history function provides a record of commands you have entered. This function is particularly useful for recalling long or complex commands or entries for the purposes of modifying them slightly and reexecuting them.

The **terminal history** command enables the command history function with the default buffer size or the last buffer size specified using the **terminal history size** command.

Table 128 lists the keys and functions you can use to recall commands from the history buffer.

Table 128 History Keys

Key(s)	Function
Ctrl-P or Up Arrow[1]	Recalls commands in the history buffer in a backward sequence, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Ctrl-N or Down Arrow[1]	Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow. Repeat the key sequence to recall successively more recent commands.

1. The arrow keys function only with ANSI-compatible terminals.

Examples

In the following example, the command history feature is disabled for the current terminal session:

```
Router> terminal no history
```

Related Commands

Command	Description
history	Enables the command history function, or changes the command history buffer size for a particular line.
show history	Lists the commands you have entered in the current EXEC session.
terminal history size	Sets the size of the history buffer for the command history feature for the current terminal session.

terminal history size

To change the size of the command history buffer for the current terminal session, use the **terminal history size** command in EXEC mode. To reset the command history buffer to its default size of 10 lines, use the **no** form of this command.

terminal history size *number-of-lines*

terminal no history size

Syntax Description

number-of-lines	Number of command lines that the system will record in its history buffer. The range is from 0 to 256. The default is 10.

Defaults

10 lines of command history

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The history feature provides a record of commands you have entered. This feature is particularly useful for recalling long or complex commands or entries for the purposes of modifying them slightly and reissuing them.

The **terminal history size** command enables the command history feature and sets the command history buffer size. The **terminal no history size** command resets the buffer size to the default of 10 command lines.

Table 129 lists the keys and functions you can use to recall commands from the history buffer. When you use these keys, the commands recalled will be from EXEC mode if you are in EXEC mode, or from all configuration modes if you are in any configuration mode.

Table 129 History Keys

Key	Function
Ctrl-P or Up Arrow[1]	Recalls commands in the history buffer in a backward sequence, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Ctrl-N or Down Arrow[1]	Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow. Repeat the key sequence to recall successively more recent commands.

1. The arrow keys function only with ANSI-compatible terminals.

In EXEC mode, you can also use the **show history** command to show the contents of the command history buffer.

To check the current settings for the command history feature on your line, use the **show line** command.

Examples

In the following example, the number of command lines recorded is set to 15 for the current terminal session. The user then checks to see what line he/she is connected to using the **show users** command. The user uses this line information to issue the show line command. (In this example, the user uses the **show begin** option in the **show line** command to start the output at the "Editing is enabled/disabled" line.)

```
Router# terminal history size 15
Router# show users

    Line       User       Host(s)              Idle       Location
* 50 vty 0     admin      idle                 00:00:00
! the * symbol indicates the active terminal session for the user (line 50)

Router# show line 50 | begin Editing

Editing is enabled.
! the following line shows the history settings for the line
History is enabled, history size is 15.
DNS resolution in show commands is enabled
Full user help is disabled
Allowed transports are telnet.  Preferred is none.
No output characters are padded
No special data dispatching characters
```

Related Commands

Command	Description
history	Enables the command history function, or changes the command history buffer size for a particular line.
show <command> begin	Searches the output of any show command and displays the output from the first instance of a specified string.
show history	Lists the commands you have entered in the current EXEC session.
terminal history	Enables the command history feature for the current terminal session.

terminal hold-character

To define the hold character for the current session, use the **terminal hold-character** command in EXEC mode. To return the hold character definition to the default, use the **no** form of this command.

terminal hold-character *ascii-number*

terminal no hold-character

Syntax Description

ascii-number	ASCII decimal representation of a character or control sequence (for example, Ctrl-P).

Defaults

The default hold character is defined by the **hold-character** global configuration command.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You can define a local hold character that temporarily suspends the flow of output on the terminal. When information is scrolling too quickly, you can enter the hold character to pause the screen output, then enter any other character to resume the flow of output.

You cannot suspend output on the console terminal. To send the hold character to the host, precede it with the escape character.

Examples

In the following example, the hold character for the current (local) session is set to Ctrl-P. The **show terminal** output is included to show the verification of the setting (the value for the hold character is shown in the "Special Characters" listing).

```
Router# terminal hold-character 16
"^P" is the local hold character
Router# show terminal
Line 50, Location: "", Type: "VT220"
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 9600/9600
Status: PSI Enabled, Ready, Active, No Exit Banner, Automore On
Capabilities: none
Modem state: Ready
Group codes:    0
Special Chars: Escape  Hold  Stop  Start  Disconnect  Activation
                ^^x     ^P    -     -       none
Timeouts:      Idle EXEC    Idle Session   Modem Answer  Session   Dispatch
               00:10:00        never                        none     not set
                            Idle Session Disconnect Warning
                              never
                            Login-sequence User Response
```

```
                              00:00:30
                             Autoselect Initial Wait
                               not set
Modem type is unknown.
Session limit is not set.
Time since activation: 00:04:13
Editing is enabled.
History is enabled, history size is 10.
.
.
.
```

Related Commands

Command	Description
hold-character	Defines the local hold character used to pause output to the terminal screen.
show terminal	Displays settings for terminal operating characteristics.

terminal international

If you are using Telnet to access a Cisco IOS platform and you want to display 8-bit and multibyte international characters (for example, Kanji) and print the Escape character as a single character instead of as the caret and bracket symbols (^[) for a current Telnet session, use the **terminal international** command in user EXEC or priviledged mode. To display characters in 7-bit format for a current Telnet session, use the **no** form of this command.

terminal international

no terminal international

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

If you are configuring a Cisco IOS platform using the Cisco web browser UI, this feature is enabled automatically when you enable the Cisco web browser UI using the **ip http server** global configuration command.

Examples

The following example enables a Cisco IOS platform to display 8-bit and multibyte characters and print the Escape character as a single character instead of as the caret and bracket symbols (^[) when you are using Telnet to access the platform for the current Telnet session:

```
Router# terminal international
```

Related Commands

Command	Description
international	Prints the Escape character as a single character instead of as the caret and bracket symbols (^[) in instances when you are using Telnet to access a Cisco IOS platform and you want to display 8-bit and multibyte international characters (for example, Kanji).

terminal keymap-type

To specify the current keyboard type for the current session, use the **terminal keymap-type** command in EXEC mode.

terminal keymap-type *keymap-name*

Syntax Description

keymap-name	Name defining the current keyboard type.

Defaults

VT100

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

You must use this command when you are using a keyboard other than the default of VT100.

Examples

The following example specifies a VT220 keyboard as the current keyboard type:

```
Router# terminal keymap-type vt220
```

Related Commands

Command	Description
show keymap	Displays the current keymap settings.

terminal length

To set the number of lines on the current terminal screen for the current session, use the **terminal length** command in EXEC mode.

terminal length *screen-length*

Syntax Description

screen-length	Number of lines on the screen. A value of zero disables pausing between screens of output.

Defaults

24 lines

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The system uses the length value to determine when to pause during multiple-screen output. A value of zero prevents the router from pausing between screens of output.

Some types of terminal sessions do not require you to specify the screen length because the screen length specified can be learned by some remote hosts. For example, the rlogin protocol uses the screen length to set up terminal parameters on a remote UNIX host.

Examples

In the following example, the system is configured to prevent output from pausing if it exceeds the length of the screen:

```
Router# terminal length 0
```

Related Commands

Command	Description
length	Sets the terminal screen length.

terminal monitor

To display **debug** command output and system error messages for the current terminal and session, use the **terminal monitor** command in EXEC mode.

terminal monitor

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Remember that all terminal parameter-setting commands are set locally and do not remain in effect after a session is ended.

Examples

In the following example, the system is configured to display **debug** command output and error messages during the current terminal session:

```
Router# terminal monitor
```

terminal notify

To enable terminal notification about pending output from other Telnet connections for the current session, use the **terminal notify** command in EXEC mode. To disable notifications for the current session, use the **no** form of this command.

terminal notify

terminal no notify

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Enabling notifications may be useful if, for example, you want to know when another connection receives mail, or when a process has been completed.

This command enables or disables notifications for only the current session. To globally set these notifications, use the **notify** line configuration command.

Examples

In the following example, notifications will be displayed to inform the user when output is pending on another connection:

```
Router# terminal notify
```

Related Commands

Command	Description
notify	Enables terminal notification about pending output from other Telnet connections.

terminal padding

To change the character padding on a specific output character for the current session, use the **terminal padding** command in EXEC mode.

terminal padding *ascii-number count*

Syntax Description

ascii-number	ASCII decimal representation of the character.
count	Number of NULL bytes sent after the specified character, up to 255 padding characters in length.

Defaults

No padding

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Character padding adds a number of null bytes to the end of the string and can be used to make a string an expected length for conformity.

Use this command when the attached device is an old terminal that requires padding after certain characters (such as ones that scrolled or moved the carriage). See the"ASCII Character Set and Hexidecimal Values" appendix for a list of ASCII characters.

Examples

The following example pads Ctrl-D (ASCII decimal character 4) with 164 NULL bytes:

```
Router# terminal padding 4 164
```

Related Commands

Command	Description
padding	Sets the padding on a specific output character.

terminal parity

To define the generation of the parity bit for the current terminal line and session, use the **terminal parity** command in EXEC mode.

terminal parity {**none** | **even** | **odd** | **space** | **mark**}

Syntax Description

none	No parity. This is the default.
even	Even parity.
odd	Odd parity.
space	Space parity.
mark	Mark parity.

Defaults

No parity.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Communication protocols provided by devices such as terminals and modems will sometimes require a specific parity bit setting. Refer to the documentation for your device to determine required parity settings.

Examples

In the following example, odd parity checking is enabled for the current session:

```
Router# terminal parity odd
```

Related Commands

Command	Description
parity	Defines generation of a parity bit for connections on a specified line or lines.

terminal rxspeed

To set the terminal receive speed (how fast information is sent to the terminal) for the current line and session, use the **terminal rxspeed** command in EXEC mode.

terminal rxspeed *bps*

Syntax Description

bps	Baud rate in bits per second (bps). The default is 9600.

Defaults

9600 bps

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Set the speed to match the baud rate of whatever device you have connected to the port. Some baud rates available on devices connected to the port might not be supported on the system. The system will indicate if the speed you select is not supported.

Examples

The following example sets the current auxiliary line receive speed to 115200 bps:

```
Router# terminal rxspeed 115200
```

Related Commands

Command	Description
rxspeed	Sets the terminal receive speed for a specified line or lines.
terminal rxspeed	Sets the terminal receive speed for the current session.
terminal txspeed	Sets the terminal transmit speed for a specified line or lines.
terminal speed	Sets the transmit and receive speeds for the current session.

terminal special-character-bits

To change the ASCII character widths to accept special characters for the current terminal line and session, use the **terminal special-character-bits** command in EXEC mode.

terminal special-character-bits {**7** | **8**}

Syntax Description

7	Selects the 7-bit ASCII character set. This is the default.
8	Selects the full 8-bit ASCII character set.

Defaults

7-bit ASCII character set

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Configuring the width to 8 bits enables you to use twice as many special characters as with the 7-bit setting. This selection enables you to add special graphical and international characters in banners, prompts, and so on.

This command is useful, for example, if you want the router to provide temporary support for international character sets. It overrides the **default-value special-character-bits** global configuration command and is used to compare character sets typed by the user with the special character available during a data connection, which includes software flow control and escape characters.

When you exit the session, character width is reset to the width established by the **default-value exec-character-bits** global configuration command.

Note that setting the EXEC character width to eight bits can cause failures. For example, if a user on a terminal that is sending parity enters the **help** command, an "unrecognized command" message appears because the Cisco IOS software is reading all eight bits, and the eighth bit is not needed for the **help** command.

Examples

The following example temporarily configures a router to use a full 8-bit user interface for system banners and prompts.

```
Router# terminal special-character-bits 8
```

Related Commands

Command	Description
default-value exec-character-bits	Globally defines the character width as 7-bit or 8-bit.
special-character-bits	Configures the number of data bits per character for special characters such as software flow control characters and escape characters.

terminal speed

To set the transmit and receive speeds of the current terminal line for the current session, use the **terminal speed** command in EXEC mode.

terminal speed *bps*

Syntax Description

bps	Baud rate in bits per second (bps). The default is 9600.

Defaults

9600 bps

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Set the speed to match the transmission rate of whatever device you have connected to the port. Some baud rates available on devices connected to the port might not be supported on the router. The router indicates whether the speed you selected is not supported.

Examples

The following example restores the transmit and receive speed on the current line to 9600 bps:

```
Router# terminal speed 9600
```

Related Commands

Command	Description
speed	Sets the terminal baud rate.

terminal start-character

To change the flow control start character for the current session, use the **terminal start-character** command in EXEC mode.

terminal start-character *ascii-number*

Syntax Description

ascii-number	ASCII decimal representation of the start character.

Defaults

Ctrl-Q (ASCII decimal character 17)

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The flow control start character signals the start of data transmission when software flow control is in effect.

Examples

The following example changes the start character to Ctrl-O (ASCII decimal character 15):

```
Router# terminal start-character 15
```

Related Commands

Command	Description
start-character	Sets the flow control start character.

terminal stopbits

To change the number of stop bits sent per byte by the current terminal line during an active session, use the **terminal stopbits** command in EXEC mode.

terminal stopbits {**1** | **1.5** | **2**}

Syntax Description

1	One stop bit.
1.5	One and one-half stop bits.
2	Two stop bits. This is the default.

Defaults

2 stop bits

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Communication protocols provided by devices such as terminals and modems often require a specific stop-bit setting.

Examples

In the following example, the setting for stop bits is changed to one for the current session:

```
Router# terminal stopbits 1
```

Related Commands

Command	Description
stopbits	Sets the number of the stop bits sent per byte.

terminal stop-character

To change the flow control stop character for the current session, use the **terminal stop-character** command in EXEC mode.

terminal stop-character *ascii-number*

Syntax Description

ascii-number	ASCII decimal representation of the stop character.

Defaults

Ctrl-S (ASCII character decimal 19)

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The flow control stop character signals the end of data transmission when software flow control is in effect.

See the "ASCII Character Set and Hexidecimal Values" appendix for a list of ASCII characters.

Examples

In the following example, the stop character is configured as Ctrl-E (ASCII character decimal 5) for the current session:

```
Router# terminal stop-character 5
```

Related Commands

Command	Description
stop-character	Sets the flow control stop character.

terminal telnet break-on-ip

To cause an access server to generate a hardware Break signal when an interrupt-process (ip) command is received, use the **terminal telnet break-on-ip** command in EXEC mode.

terminal telnet break-on-ip

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The hardware Break signal occurs when a Telnet interrupt-process (ip) command is received on that connection. The **terminal telnet break-on-ip** command can be used to control the translation of Telnet interrupt-process commands into X.25 Break indications.

Note In this command, the acronym "ip" indicates "interrupt-process," not Internet Protocol (IP).

This command is also a useful workaround in the following situations:

- Several user Telnet programs send an ip command, but cannot send a Telnet Break signal.
- Some Telnet programs implement a Break signal that sends an ip command.

Some EIA/TIA-232 hardware devices use a hardware Break signal for various purposes. A hardware Break signal is generated when a Telnet Break command is received.

You can verify if this command is enabled with the **show terminal** EXEC command. If enabled the following line will appear in the output: `Capabilities: Send BREAK on IP`.

Examples

In the following example, a Break signal is generated for the current connection when an interrupt-process command is issued:

```
Router# terminal telnet break-on-ip
```

Related Commands

Command	Description
terminal telnet ip-on-break	Configures the system to send an interrupt-process (ip) signal when the Break command is issued.

terminal telnet refuse-negotiations

To configure the current session to refuse to negotiate full-duplex, remote echo options on incoming connections, use the **terminal telnet refuse-negotiations** command in EXEC mode.

terminal telnet refuse-negotiations

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You can set the line to allow access server to refuse full-duplex, remote echo connection requests from the other end. This command suppresses negotiation of the Telnet Remote Echo and Suppress Go Ahead options.

Examples

In the following example, the current session is configured to refuse full-duplex, remote echo requests:

```
Router# terminal telnet refuse-negotiations
```

terminal telnet speed

To allow an access server to negotiate transmission speed for the current terminal line and session, use the **terminal telnet speed** command in EXEC mode.

terminal telnet speed *default-speed maximum-speed*

Syntax Description

default-speed	Line speed, in bits per second (bps), that the access server will use if the device on the other end of the connection has not specified a speed.
maximum-speed	Maximum line speed in bits per second (bps), that the device on the other end of the connection can use.

Defaults

9600 bps (unless otherwise set using the **speed**, **txspeed** or **rxspeed** line configuration commands)

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You can match line speeds on remote systems in reverse Telnet, on host machines connected to an access server to access the network, or on a group of console lines connected to the access server when disparate line speeds are in use at the local and remote ends of the connections listed above. Line speed negotiation adheres to the Remote Flow Control option, defined in RFC 1080.

Note This command applies only to access servers. It is not supported on standalone routers.

Examples

The following example enables the access server to negotiate a bit rate on the line using the Telnet option. If no speed is negotiated, the line will run at 2400 bps. If the remote host requests a speed greater than 9600 bps, then 9600 bps will be used.

```
Router# terminal telnet speed 2400 9600
```

terminal telnet sync-on-break

To cause the access server to send a Telnet Synchronize signal when it receives a Telnet Break signal on the current line and session, use the **terminal telnet sync-on-break** command in EXEC mode.

terminal telnet sync-on-break

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You can configure the session to cause a reverse Telnet line to send a Telnet Synchronize signal when it receives a Telnet Break signal. The TCP Synchronize signal clears the data path, but still interprets incoming commands.

Note This command applies only to access servers. It is not supported on standalone routers.

Examples

The following example sets an asynchronous line to cause the access server to send a Telnet Synchronize signal:

```
Router# terminal telnet sync-on-break
```

terminal telnet transparent

To cause the current terminal line to send a Return character (CR) as a CR followed by a NULL instead of a CR followed by a Line Feed (LF) for the current session, use the **terminal telnet transparent** command in EXEC mode.

terminal telnet transparent

Syntax Description

This command has no arguments or keywords.

Defaults

CR followed by an LF

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The end of each line typed at the terminal is ended with a Return (CR). This command permits interoperability with different interpretations of end-of-line demarcation in the Telnet protocol specification.

Note This command applies only to access servers. It is not supported on stand-alone routers.

Examples

In the following example, the session is configured to send a CR signal as a CR followed by a NULL:

```
Router# terminal telnet transparent
```

terminal terminal-type

To specify the type of terminal connected to the current line for the current session, use the **terminal terminal-type** command in EXEC mode.

terminal terminal-type *terminal-type*

Syntax Description

terminal-type	Defines the terminal name and type, and permits terminal negotiation by hosts that provide that type of service. The default is VT100.

Defaults

VT100

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Indicate the terminal type if it is different from the default of VT100.

The terminal type name is used by TN3270s for display management and by Telnet and rlogin to inform the remote host of the terminal type.

Examples

In the following example, the terminal type is defined as VT220 for the current session:

```
Router# terminal terminal-type VT220
```

Related Commands

Command	Description
terminal keymap-type	Specifies the current keyboard type for the current session.
terminal-type	Specifies the type of terminal connected to a line.

terminal txspeed

To set the terminal transmit speed (how fast the terminal can send information) for the current line and session, use the **terminal txspeed** command in EXEC mode.

terminal txspeed *bps*

Syntax Description

bps	Baud rate in bits per second (bps). The default is 9600 bps.

Defaults

9600 bps

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

In the following example, the line transmit speed is set to 2400 bps for the current session:

```
Router# terminal txspeed 2400
```

Related Commands

Command	Description
rxspeed	Sets the terminal receive speed for a specified line or lines.
terminal rxspeed	Sets the terminal receive speed for the current line and session.
terminal terminal-type	Specifies the type of terminal connected to the current line for the current session.
txspeed	Sets the terminal transmit speed for a specified line or lines.

terminal width

To set the number of character columns on the terminal screen for the current line for a session, use the **terminal width** command in EXEC mode.

terminal width *characters*

Syntax Description

characters	Number of character columns displayed on the terminal. The default is 80 characters.

Defaults

80 characters

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

By default, the route provides a screen display width of 80 characters. You can reset this value for the current session if it does not meet the needs of your terminal.

The rlogin protocol uses the value of the *characters* argument to set up terminal parameters on a remote host.

Examples

The following example sets the terminal character columns to 132:

```
Router# terminal width 132
```

Related Commands

Command	Description
width	Sets the terminal screen width (the number of character columns displayed on the attached terminal).

terminal-queue entry-retry-interval

To change the retry interval for a terminal port queue, use the **terminal-queue entry-rety-interval** command in global configuration mode. To restore the default terminal port queue interval, use the **no** form of this command.

terminal-queue entry-retry-interval *seconds*

no terminal-queue entry-retry-interval

Syntax Description

seconds	Number of seconds between terminal port retries. The default is 60 seconds.

Defaults

60 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

If a remote device (such as a printer) is busy, the connection attempt is placed in a terminal port queue. If you want to decrease the waiting period between subsequent connection attempts, decrease the default of 60 to an interval of 10 seconds. Decrease the time between subsequent connection attempts when, for example, a printer queue stalls for long periods.

Examples

The following example changes the terminal port queue retry interval from the default of 60 seconds to 10 seconds:

```
Router# terminal-queue entry-retry-interval 10
```

terminal-type

To specify the type of terminal connected to a line, use the **terminal-type** command in line configuration mode. To remove any information about the type of terminal and reset the line to the default terminal emulation, use the **no** form of this command.

terminal-type {*terminal-name* | *terminal-type*}

no terminal-type

Syntax Description

terminal-name	Terminal name.
terminal-type	Terminal type.

Defaults

VT100

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command records the type of terminal connected to the line. The *terminal-name* argument provides a record of the terminal type and allows terminal negotiation of display management by hosts that provide that type of service.

For TN3270 applications, this command must follow the corresponding ttycap entry in the configuration file.

Examples

The following example defines the terminal on line 7 as a VT220:

```
Router(config)# line 7
Router(config-line)# terminal-type VT220
```

test flash

To test Flash memory on MCI and envm Flash EPROM interfaces, use the **test flash** command in EXEC mode.

test flash

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

In the following example, the Flash memory is tested:

```
test flash
```

Related Commands

Command	Description
test interfaces	Tests the system interfaces on the modular router.
test memory	Performs a test of Multibus memory (including nonvolatile memory) on the modular router.

test interfaces

To test the system interfaces on the modular router, use the **test interfaces** command in EXEC mode.

test interfaces

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **test interfaces** EXEC command is intended for the factory checkout of network interfaces. It is not intended for diagnosing problems with an operational router. The **test interfaces** output does not report correct results if the router is attached to a "live" network. For each network interface that has an IP address that can be tested in loopback (MCI and ciscoBus Ethernet and all serial interfaces), the **test interfaces** command sends a series of ICMP echoes. Error counters are examined to determine the operational status of the interface.

Examples

In the following example, the system interfaces are tested:

```
test interfaces
```

Related Commands

Command	Description
test flash	Tests Flash memory on MCI and envm Flash EPROM interfaces.
test memory	Performs a test of Multibus memory (including nonvolatile memory) on the modular router.

test memory

To perform a test of Multibus memory (including nonvolatile memory) on the modular router, use the **test memory** command in EXEC mode. The memory test overwrites memory.

test memory

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The memory test overwrites memory. If you use the **test memory** command, you will need to rewrite nonvolatile memory. For example, if you test Multibus memory, which is the memory used by the CSC-R 4-Mbps Token Ring interfaces, you will need to reload the system before the network interfaces will operate properly. The **test memory** command is intended primarily for use by Cisco personnel.

Examples

In the following example, the memory is tested:

```
test memory
```

Related Commands

Command	Description
test flash	Tests Flash memory on MCI and envm Flash EPROM interfaces.
test interfaces	Tests the system interfaces on the modular router.

tftp-server

To configure a router or a Flash memory device on the router as a TFTP server, use one of the following **tftp-server** commands in global configuration mode. This command replaces the **tftp-server system** command. To remove a previously defined filename, use the **no** form of this command with the appropriate filename.

tftp-server flash [*partition-number***:**]*filename1* [**alias** *filename2*] [*access-list-number*]

tftp-server rom alias *filename1* [*access-list-number*]

no tftp-server {**flash** [*partition-number***:**]*filename1* | **rom alias** *filename2*}

Cisco 1600 Series and Cisco 3600 Series Routers

tftp-server flash [*device***:**][*partition-number***:**]*filename*

no tftp-server flash [*device***:**][*partition-number***:**]*filename*

Cisco 7000 Family Routers

tftp-server flash *device***:***filename*

no tftp-server flash *device***:***filename*

Syntax Description

flash	Specifies TFTP service of a file in Flash memory.
rom	Specifies TFTP service of a file in ROM.
filename1	Name of a file in Flash or in ROM that the TFTP server uses in answering TFTP Read Requests.
alias	Specifies an alternate name for the file that the TFTP server uses in answering TFTP Read Requests.
filename2	Alternate name of the file that the TFTP server uses in answering TFTP Read Requests. A client of the TFTP server can use this alternate name in its Read Requests.
access-list-number	(Optional) Basic IP access list number. Valid values are from 0 to 99.
*partition-number***:**	(Optional) Specifies TFTP service of a file in the specified partition of Flash memory. If the partition number is not specified, the file in the first partition is used. For the Cisco 1600 series and Cisco 3600 series routers, you must enter a colon after the partition number if a filename follows it.

device:	(Optional) Specifies TFTP service of a file on a Flash memory device in the Cisco 1600 series, Cisco 3600 series, and Cisco 7000 family routers. The colon is required. Valid devices are as follows: • **flash**—Internal Flash memory on the Cisco 1600 series and Cisco 3600 series routers. This is the only valid device for the Cisco 1600 series routers. • **bootflash**—Internal Flash memory in the Cisco 7000 family routers. • **slot0**—First PCMCIA slot on the Cisco 3600 series and Cisco 7000 family routers. • **slot1**—Second PCMCIA slot on the Cisco 3600 series and Cisco 7000 family. • **slavebootflash**—Internal Flash memory on the slave RSP card of a Cisco 7507 or Cisco 7513 router configured for HSA. • **slaveslot0**—First PCMCIA slot of the slave RSP card on a Cisco 7507 or Cisco 7513 router configured for HSA. • **slaveslot1**—Second PCMCIA slot of the slave RSP card on a Cisco 7507 or Cisco 7513 router configured for HSA.
filename	Name of the file on a Flash memory device that the TFTP server uses in answering a TFTP Read Request. Use this argument only with the Cisco 1600 series, Cisco 3600 series, Cisco 7000 series, or Cisco 7500 series routers.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

You can specify multiple filenames by repeating the **tftp-server** command. The system sends a copy of the system image contained in ROM or one of the system images contained in Flash memory to any client that issues a TFTP Read Request with this filename.

If the specified *filename1* or *filename2* argument exists in Flash memory, a copy of the Flash image is sent. On systems that contain a complete image in ROM, the system sends the ROM image if the specified *filename1* or *filename2* argument is not found in Flash memory.

Images that run from ROM cannot be loaded over the network. Therefore, it does not make sense to use TFTP to offer the ROMs on these images.

On the Cisco 7000 family routers, the system sends a copy of the file contained on one of the Flash memory devices to any client that issues a TFTP Read Request with its filename.

Examples

In the following example, the system uses TFTP to send a copy of the *version-10.3* file located in Flash memory in response to a TFTP Read Request for that file. The requesting host is checked against access list 22.

```
tftp-server flash version-10.3 22
```

In the following example, the system uses TFTP to send a copy of the ROM image *gs3-k.101* in response to a TFTP Read Request for the gs3-k.101 file:

```
tftp-server rom alias gs3-k.101
```

In the following example, the system uses TFTP to send a copy of the *version-11.0* file in response to a TFTP Read Request for that file. The file is located on the Flash memory card inserted in slot 0.

```
tftp-server flash slot0:version-11.0
```

The following example enables a Cisco 3600 series router to operate as a TFTP server. The source file c3640-i-mz is in the second partition of internal Flash memory.

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
router(config)# tftp-server flash flash:2:dirt/gate/c3640-i-mz
```

In the following example, the source file is in the second partition of the Flash memory PC card in slot 0 on a Cisco 3600 series:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# tftp-server flash slot0:2:dirt/gate/c3640-j-mz
```

The following example enables a Cisco 1600 series router to operate as a TFTP server. The source file c1600-i-mz is in the second partition of Flash memory:

```
router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
router(config)# tftp-server flash flash:2:dirt/gate/c1600-i-mz
```

Related Commands

Command	Description
access-list	Creates an extended access list.

tftp-server system

The **tftp-server system** command has been replaced by the **tftp-server** command. See the description of the **tftp-server** command in this chapter for more information.

threshold

To set the rising threshold (hysteresis) that generates a reaction event and stores history information for the Service Assurance Agent (SAA) operation, use the **threshold** command in SAA RTR configuration mode. To return to the default value, use the **no** form of this command.

threshold *milliseconds*

no threshold

Syntax Description

milliseconds	Number of milliseconds required for a rising threshold to be declared. The default value is 5000 ms.

Defaults

5000 ms

Command Modes

SAA RTR configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The value specified for the **threshold** command must not exceed the value specified for the **timeout** SAA RTR configuration command.

The threshold value is used by the **rtr reaction-configuration** and **filter-for-history** commands.

Examples

In the following example, the threshold of operation 1 is set to 2500 ms:

```
Router(config)# rtr 1
Router(config-rtr)# type echo protocol ipIcmpEcho 172.16.1.176
Router(config-rtr)# threshold 2500
```

Related Commands

Command	Description
filter-for-history	Defines the type of information kept in the history table for the SAA operation.
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.
rtr reaction-configuration	Configures certain actions to occur based on events under the control of the SAA.

timeout

To set the amount of time the Service Assurance Agent (SAA) operation waits for a response from its request packet, use the **timeout** command in SAA RTR configuration mode. To return to the default value, use the **no** form of this command.

timeout *milliseconds*

no timeout

Syntax Description

milliseconds	Number of milliseconds (ms) the operation waits to receive a response from its request packet.

Defaults

The default timeout values vary by operation. Per the RTTMON-MIB, the defaults are:

DLSw+ (type dlsw) and FTP (type ftp) operations: 30000 ms

DNS (type dns) operations: 9 seconds
(as defined by multiplying the MAX_DNS_WAITTIME value by the MAXDNSTRIES value)

TCP Connection (type tcpConnect) and HTTP (type http) operations: 60 seconds
(as defined by multiplying the MAXALIVETRIES value by the MAXSYNTRYTICKS value)

Command Modes

SAA RTR configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use the **timeout** command to set how long the operation waits to receive a response, and use the **frequency** SAA RTR configuration command to set the rate at which the SAA starts an operation.

The value specified for the **timeout** command cannot be greater than the value specified for the **frequency** command.

Examples

In the following example, the timeout for the IP/ICMP Echo operation 1 is set for 2500 ms:

```
Router(config)# rtr 1
Router(config-rtr)# type echo protocol ipIcmpEcho 172.16.1.176
Router(config-rtr)# timeout 2500
```

Related Commands

Command	Description
frequency	Sets the rate at which the SAA operation starts a response time operation.
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.

time-range

To enable time-range configuration mode and define time ranges for functions (such as extended access lists), use the **time-range** command in global configuration mode. To remove the time limitation, use the **no** form of this command.

time-range *time-range-name*

no time-range *time-range-name*

Syntax Description

time-range-name	Desired name for the time range. The name cannot contain a space or quotation mark, and must begin with a letter.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.

Usage Guidelines

The **time-range** entries are identified by a name, which is referred to by one or more other configuration commands. Multiple time ranges can occur in a single access list or other feature.After the **time-range** command, use the **periodic** time-range configuration command, the **absolute** time-range configuration command, or some combination of them to define when the feature is in effect. Multiple **periodic** commands are allowed in a time range; only one **absolute** command is allowed.

Tips To avoid confusion, use different names for time ranges and named access lists.

Examples

The following example denies HTTP traffic on Monday through Friday from 8:00 a.m. to 6:00 p.m. The example allows UDP traffic on Saturday and Sunday from noon to midnight only.

```
time-range no-http
 periodic weekdays 8:00 to 18:00
!
time-range udp-yes
 periodic weekend 12:00 to 24:00
!
ip access-list extended strict
 deny tcp any any eq http time-range no-http
 permit udp any any time-range udp-yes
!
interface ethernet 0
 ip access-group strict in
```

Related Commands

Command	Description
absolute	Specifies an absolute start and end time for a time range.
ip access-list	Defines an IP access list by name.
periodic	Specifies a recurring (weekly) start and end time for a time range.
permit (IP)	Sets conditions under which a packet passes a named IP access list.

tos

To define a type of service (ToS) byte in the IP header of Service Assurance Agent (SAA) operations, use the **tos** command in SAA RTR configuration mode. To return to the default value, use the **no** form of this command.

tos *number*

no tos

Syntax Description

number	Service type byte in the IP header. The range is 0 to 255. The default is 0.

Defaults

The default type-of-service value is 0.

Command Modes

SAA RTR configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

The ToS value is an 8-bit field in IP headers. This field contains information such as precedence and TOS. This is useful for policy-routing as well as features like Committed Access Rate (CAR) , where routers examine for TOS values.

When the type-of-service is defined for an operation, the SAA Responder will reflect the ToS value it recieves.

Examples

In the following example, SAA operation 1 is configured as an echo probe using the IP/ICMP Echo protocol and the destination IP address 172.16.1.175. The ToS value is set to 0x80.

```
Router(config)# rtr 1
Router(config-rtr)# type echo protocol ipIcmpEcho 172.16.1.176
Router(config-rtr)# tos 0x80
```

Related Commands

Command	Description
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.

traceroute

To discover the routes that packets will actually take when traveling to their destination address, use the **traceroute** command in user EXEC or privileged EXEC mode.

traceroute [**vrf** *vrf-name*] [*protocol*] *destination*

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name of a Virtual Private Network (VPN) routing/forwarding instance table (VRF) in which to find the destination address. The only *protocol* argument keyword that you can select when you use the **vrf** *vrf-name* keyword-argument pair is the **ip** keyword.
protocol	(Optional) Protocol keyword, either **appletalk**, **clns**, **ip**, **ipv6**, **ipx**, **oldvines**, or **vines**. When not specified, the *protocol* argument is based on an examination by the software of the format of the *destination* argument.
destination	(Optional in privileged EXEC mode; required in user EXEC mode) The destination address or host name for which you want to trace the route. The software determines the default parameters for the appropriate protocol and the tracing action begins.

Defaults

When not specified, the protocol argument is determined by the software examining the format of the *destination* argument. For example, if the software finds a *destination* argument in IP format, the protocol value defaults to IP.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	The **vrf** *vrf-name* keyword and argument were added.
12.2(2)T, 12.0(21)ST, 12.0(22)S	Support for IPv6 was added.
12.2(11)T	The **traceroute** command test characters for IPv6 were updated. A new error message was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(5), 12.0(26)S1, 12.2(20)S	A line was added to the interactive **traceroute vrf** command, so that you can resolve the autonomous system (AS) number through the use of the global table or a VRF table, or you can choose not to resolve the AS.

Usage Guidelines

The **traceroute** command works by taking advantage of the error messages generated by routers when a datagram exceeds its hop limit value.

The **traceroute** command starts by sending probe datagrams with a hop limit of 1. Including a hop limit of 1 with a probe datagram causes the neighboring routers to discard the probe datagram and send back an error message. The **traceroute** command sends several probes with increasing hop limits and displays the round-trip time for each.

The **traceroute** command sends out one probe at a time. Each outgoing packet might result in one or more error messages. A time-exceeded error message indicates that an intermediate router has seen and discarded the probe. A destination unreachable error message indicates that the destination node has received and discarded the probe because the hop limit of the packet reached a value of 0. If the timer goes off before a response comes in, the **traceroute** command prints an asterisk (*).

The **traceroute** command terminates when the destination responds, when the hop limit is exceeded, or when the user interrupts the trace with the escape sequence. By default, to invoke the escape sequence, type **Ctrl-^ X**—by simultaneously pressing and releasing the **Ctrl**, **Shift**, and **6** keys, and then pressing the **X** key.

To use nondefault parameters and invoke an extended **traceroute** test, enter the command without a *protocol* or *destination* argument in privileged EXEC mode. You are stepped through a dialog to select the desired parameters. Extended **traceroute** tests are not supported in user EXEC mode. The user-level traceroute feature provides a basic trace facility for users who do not have system privileges. The *destination* argument is required in user EXEC mode.

If the system cannot map an address for a host name, it returns a "%No valid source address for destination" message.

Resolving the AS with Interactive VRF Traceroute

In the noninteractive mode, the **traceroute vrf** command always resolves the AS in the global routing table. A destination address is required when you use the noninteractive command. Here, for example, the address is 10.0.0.3.

```
Router# traceroute vrf green 10.0.0.3
```

In the interactive mode, a line in the **traceroute vrf** command allows you to select the global routing table or VRF table to resolve the AS number of a host address or to choose not to resolve the AS:

```
Resolve AS number in (G)lobal table, (V)RF or(N)one [G]:
```

If you do not select one of these options to resolve the AS, the AS is resolved in the global routing table (default behavior).

The following example shows you the line where you select the routing table option that best represents the configuration of your network:

```
Router# traceroute vrf green

Protocol [ip]:
Target IP address:  10.0.0.3
Source address:
Numeric display [n]:
Resolve AS number in (G)lobal table, (V)RF or(N)one [G]:VRF
Timeout in seconds [3]:
. . .
```

Note IP is the only protocol that you can select for a destination address when you use the **traceroute vrf** command.

If you select **N(one)**, the AS is not resolved, and the AS is not indicated in the output of the command. For example:

```
Tracing the route to 10.0.0.3
```

```
  1 10.1.1.9 [MPLS: Labels 25/45 Exp 0] 4 msec 0 msec 0 msec
  2 10.1.1.1 [MPLS: Labels 26/45 Exp 0] 0 msec 4 msec 0 msec
  3 10.12.1.101 [MPLS: Labels 23/45 Exp 0] 0 msec 0 msec 0 msec
  4 10.12.1.6 [MPLS: Labels 19/45 Exp 0] 4 msec 0 msec 0 msec
  5 10.12.1.41 [MPLS: Label 45 Exp 0] 0 msec 4 msec 0 msec
  6 10.12.1.42 0 msec 0 msec 0 msec
  7 10.0.0.3 4 msec *  0 msec
```

If you select (**V)RF**, the AS is resolved in the VRF table, and the AS is indicated in the output of the command. For example:

```
Tracing the route to 10.0.0.3

  1 10.1.1.9 [AS 100] [MPLS: Labels 25/45 Exp 0] 0 msec 4 msec 0 msec
  2 10.1.1.1 [AS 100] [MPLS: Labels 26/45 Exp 0] 0 msec 0 msec 0 msec
  3 10.12.1.101 [AS 100] [MPLS: Labels 23/45 Exp 0] 4 msec 0 msec 0 msec
  4 10.12.1.6 [AS 100] [MPLS: Labels 19/45 Exp 0] 0 msec 4 msec 0 msec
  5 10.12.1.41 [AS 100] [MPLS: Label 45 Exp 0] 0 msec 0 msec 4 msec
  6 10.12.1.42 [AS 100] 0 msec 0 msec 0 msec
  7 10.0.0.3 [AS 100] 0 msec *  0 msec
```

The path from a provider edge (PE)1 router to a PE2 router might contain routes from the global routing table and a VRF table. If that happens, you need to enter two interactive **traceroute vrf** commands at the PE1 router to trace the route to a customer edge (CE)2 router: one selecting the global routing table, and the other selecting a VRF table. You can then determine the valid and invalid AS numbers based on your knowledge of the network topology. In an interautonomous system (Inter-AS) network, however, you might not know the whole topology.

Common Traceroute Problems

Due to bugs in the IP implementation of various hosts and routers, the IP **traceroute** command might behave in an unexpected manner.

Not all destinations respond correctly to a probe message by sending back an “ICMP port unreachable” message. A long sequence of asterisks, terminating only when the maximum hop limit has been reached, might indicate this problem.

There is a known problem with the way some hosts handle an “ICMP TTL exceeded” message. Some hosts generate an “ICMP” message, but they reuse the Time to Live (TTL) of the incoming packet. Because the TTL of the incoming packet is 0, the Internet Control Message Protocol (ICMP) packets do not make it back. When you trace the path to such a host, you might see a set of TTL values with asterisks (*). Eventually the hop limit gets high enough that the “*ICMP”* message can get back. For example, if the host is six hops away, traceroute times out on responses 6 through 11.

Note In IPv4, the TTL value can be an amount of time (for example, 250 milliseconds) or a hop count. In IPv6, the equivalent of the TTL value is always a hop count.

Examples

The following user EXEC example shows the IPv4 **traceroute** output that results when a destination host name has been specified:

```
Router> traceroute host77-name.domainZZ-name.com

Type escape sequence to abort.
Tracing the route to host77-name.domainZZ-name.com (10.0.0.73)
  1 host1-name.domain1-name.com (192.168.1.6) 1000 msec 8 msec 4 msec
  2 host33-name.serviceprovider8-name.com (192.168.16.2) 8 msec 8 msec 8 msec
  3 host2-name.college2-name.edu (192.168.110.225) 8 msec 4 msec 4 msec
```

```
  4 host44-name.domain2-name.NET (192.168.254.6) 8 msec 8 msec 8 msec
  5 host22-name.serviceprovider99-name.com (192.168.3.8) 12 msec 12 msec 8 msec
  6 host-name5.domain5-name.com (192.168.195.1) 216 msec 120 msec 132 msec
  7 host77-name.domainZZ-name.com (10.0.0.73) 412 msec 628 msec 664 msec
```

Table 130 describes the significant fields shown in the display.

Table 130 traceroute Field Descriptions When IPv4 Is Used

Field	Description
1	Indicates the sequence number of the router in the path to the host
host1-name.domain1-name.com	Host name of this router
192.168.1.6	Internet address of this router
1000 msec 8 msec 4 msec	Round-trip time for each of the three transmitted probes

The following user EXEC example shows the IPv6 **traceroute** output that results when a destination host name has been specified:

```
Router> traceroute host8-name.domainBB-name.no

Type escape sequence to abort.
Tracing the route to host8-name.domainBB-name.no (3FFE:2A00:100:7FF9::2)
  1 3FFE:C:00:E:13::2 28 msec 24 msec *
  2 3FFE:2A00:100:7FF8::2 208 msec 204 msec
  3 host32-name.domainHH-name.net (3FFE:2A00:100:7FF8::1) 276 msec * 276 msec
  4 host8-name.domainBB-name.no (3FFE:2A00:100:7FF9::2) 292 msec 292 msec 296 msec
```

Note In the example, host8-name.domainBB-name.no has an IPv6 address, so the protocol for the **traceroute** command defaults to IPv6. IPv4 could be used if you specify **ip** in the **traceroute** command; for example, **traceroute ip host8-name.domainBB-name.no**.

Table 131 describes the significant fields shown in the display.

Table 131 traceroute Field Descriptions When IPv4 Is Used

Field	Description
4	Indicates the sequence number of the router in the path to the host
host8-name.domainBB-name.no	Host name of the destination node
3FFE:2A00:100:7FF9::2	IPv6 address of the destination node
292 msec 292 msec 296 msec	Round-trip time for each of the three transmitted probes

The following privileged EXEC example shows the extended dialog of the **traceroute** command when IPv4 is used:

```
Router# traceroute

Protocol [ip]:
Target IP address: host77-name.domainZZ-name.com
Source address:
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
```

```
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to host77-name.domainZZ-name.com (10.0.0.73)
  1 host1-name.domain1-name.com (192.168.1.6) 1000 msec 8 msec 4 msec
  2 host33-name.serviceprovider8-name.com (192.168.16.2) 8 msec 8 msec 8 msec
  3 host2-name.college2-name.edu (192.168.110.225) 8 msec 4 msec 4 msec
  4 host44-name.domain2-name.NET (192.168.254.6) 8 msec 8 msec 8 msec
  5 host22-name.serviceprovider99-name.com (192.168.3.8) 12 msec 12 msec 8 msec
  6 host-name5.domain5-name.com (192.168.195.1) 216 msec 120 msec 132 msec
  7 host77-name.domainZZ-name.com (10.0.0.73) 412 msec 628 msec 664 msec
```

If an unknown host name is used in the Target IP address field, the software queries a Domain Name System (DNS) server to resolve the unknown host name to its IP address. In the following example, a DNS server (IP address 192.168.7.93) is queried for the unknown host name college9-name.edu:

```
Router# traceroute

Protocol [ip]:
Target IP address: college9-name.edu
Translating "college9-name.edu"...domain server (192.168.7.93) [OK]
```

Table 132 describes the fields that are unique to the extended traceroute sequence that is shown in the display.

Table 132 traceroute Field Descriptions When IPv4 Is Used

Field	Description
Target IP address	You must enter an IPv4 host name or an IPv4 address. There is no default.
Source address	One of the interface addresses of the router to use as a source address for the probes. The router normally chooses what it considers to be the best source address.
Numeric display	The default is to have both a symbolic and numeric display; however, you can suppress the symbolic display.
Timeout in seconds	The number of seconds to wait for a response to a probe packet. The default is 3 seconds.
Probe count	The number of probes to be sent at each TTL level. The default count is 3.
Minimum Time to Live [1]	The TTL value for the first probes. The default is 1, but it can be set to a higher value to suppress the display of known hops.
Maximum Time to Live [30]	The largest TTL value that can be used. The default is 30. The command terminates when the traceroute packet reaches the destination or when the value is reached.
Port Number	The destination port used by the User Datagram Protocol (UDP) probe messages. The default is 33434.
Loose, Strict, Record, Timestamp, Verbose	IP header options. You can specify any combination. The command issues prompts for the required fields. The command also places the requested options in each probe; however, there is no guarantee that all routers (or end nodes) will process the options.
Loose	Allows you to specify a list of nodes that the traceroute packet must traverse to the destination.

Table 132 traceroute Field Descriptions When IPv4 Is Used (continued)

Field	Description
Strict	Allows you to specify a list of nodes that must be the only nodes traversed when the traceroute packet goes to the destination.
Record	Allows you to specify the number of hops.
Timestamp	Allows you to specify the number of time stamps.
Verbose	If you select any option, the verbose mode is automatically selected, and the command prints the contents of the option field in any incoming packets. You can prevent verbose mode by selecting it again and toggling its current setting.

The following privileged EXEC example shows the extended dialog of the **traceroute** command when IPv6 is used:

```
Router# traceroute

Protocol [ip]: ipv6
Target IP address: host8-name.domainBB-name.no
Source IPv6 address:
Numeric display [no]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Priority [0]:
Port Number [33434]:
Type escape sequence to abort.
Tracing the route to host8-name.domainBB-name.no (3FFE:2A00:100:7FF9::2)
  1 3FFE:C:00:E:13::2 28 msec 24 msec *
  2 3FFE:2A00:100:7FF8::2 208 msec 204 msec
  3 host32-name.domainHH-name.net (3FFE:2A00:100:7FF8::1) 276 msec * 276 msec
  4 host8-name.domainBB-name.no (3FFE:2A00:100:7FF9::2) 292 msec 292 msec 296 msec
```

If an unknown host name is used in the Target IP address field, software queries a DNS server to resolve the unknown host name to an IP address. In the following example, a DNS server (IP address 192.168.7.93) is queried for the unknown host name host8-name.domainBB-name.no:

```
Router# traceroute

Protocol [ip]: ipv6
Target IP address: host8-name.domainBB-name.no
Translating "host8-name.domainBB-name.no"...domain server (192.168.7.93) [OK]
```

Table 133 describes the fields that are unique to the extended **traceroute** sequence shown in the display.

Table 133 traceroute Field Descriptions When IPv4 Is Used

Field	Description
Protocol [ip]:	The protocol to use for the probes. The available protocols are **appletalk**, **clns**, **ip**, **ipv6**, **ipx**, **oldvines**, and **vines**. The default is **ip**.
Target IP address	You must enter an IPv6 host name or an IPv6 address. There is no default.

Table 133 traceroute Field Descriptions When IPv4 Is Used (continued)

Field	Description
Source IPv6 address	The IPv6 address of an interface in the router that is used as the source address for the probes. If you do not enter an address, the router chooses what it considers to be the best source address. **Note** In Cisco IOS Release 12.2(8)T and later releases, an IPv6 address enclosed in square brackets ([ ]), such as [FE80::260:3EFF:FE11:6770], is acceptable to the system. Refer to RFC 2732, *Format for Literal IPv6 Addresses in URL's*, for more information on the use of square brackets with literal IPv6 addresses as in URLs.
Numeric display	The default is to have both a symbolic and numeric display; however, you can suppress the symbolic display.
Timeout in seconds	The number of seconds to wait for a response to a probe packet. The default is 3 seconds.
Probe count	The number of probes to be sent at each TTL level. The default count is 3.
Minimum Time to Live [1]	The HopCount (TTL) value or hop limit for the first probes. The default is 1, but it can be set to a higher value if you want to suppress the display of known hops.
Maximum Time to Live [30]	The largest HopCount (TTL) value or hop limit that can be used. The default is 30. The command terminates when the traceroute packet reaches the destination or when this value is reached.
Port Number	The destination port used by the UDP probe messages. The default is 33434.

Table 134 describes the characters that can appear in **traceroute** command output when IPv4 is used.

Table 134 traceroute Text Characters When IPv4 Is Used

Character	Description
nn msec	For each node, the round-trip time (in milliseconds) for the specified number of probes.
*	The probe timed out. No response was received within the specified period.
?	Unknown error.
A	Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.
H	Host unreachable.
N	Network unreachable (beyond scope).
P	Protocol unreachable.
Q	Source quench.
P	Port unreachable.

Table 135 describes the characters that can appear in the **traceroute** command output when IPv6 is used.

Table 135 traceroute Text Characters When IPv6 Is Used

Character	Description
!	Indicates receipt of a reply.
*	The probe timed out. No response was received within the specified period.
?	Unknown error.
@	Unreachable for unknown reason.
A	Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.
H	Host unreachable.
N	Network unreachable (beyond scope).
P	Port unreachable.
U	No route to host.

transport event

To specify that inventory events are sent out by the CNS inventory agent, use the **transport event** command in CNS inventory configuration mode. To disable the transport of inventory events, use the **no** form of this command.

transport event

no transport event

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

CNS inventory configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use this command to send out inventory requests with each CNS inventory agent message. When configured, the routing device will respond to queries from the CNS Event Bus. Online insertion and removal (OIR) events on the routing device will be reported to the CNS Event Bus.

Examples

The following example shows how to enable the CNS inventory agent and configure it to send out inventory events:

```
Router(config)# cns inventory
Router(cns_inv)# transport event
```

Related Commands

Command	Description
cns inventory	Enables the CNS inventory agent and enters CNS inventory configuration mode.

ttl dns

To configure the number of seconds for which an answer received from the boomerang client will be cached by the Domain Name System (DNS) client, use the **ttl dns** command in boomerang configuration mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

ttl dns *seconds*

no ttl dns *seconds*

Syntax Description

seconds	Number of seconds for which an answer received from the boomerang client will be cached by the DNS client. Range is from 10 to 2147483647.

Defaults

No default behavior or values.

Command Modes

Boomerang configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

The **ttl dns** command can be used only on a Director Response Protocol (DRP) agent. The boomerang client is the DRP agent.

The **ttl dns** command configures the number of seconds for which the DNS client can cache a boomerang reply from a boomerang client.

Examples

In the following example, the number of seconds for which the DNS client can cache a boomerang reply from a boomerang client is configured as 10:

```
Router(config)# ip drp domain www.boom1.com
Router(config-boomerang)# ttl dns 10

Router# show running-config
.
.
.
ip drp domain www.boom1.com
dns-ttl 10
```

Related Commands

Command	Description
alias (boomerang configuration)	Configures an alias name for a specified domain.
ip drp domain	Adds a new domain to the DistributedDirector client or configures an existing domain and puts the client in boomerang configuration mode.
server (boomerang configuration)	Configures the server address for a specified boomerang domain.
show ip drp	Displays DRP statistics on DistributedDirector or a DRP server agent.
show ip drp boomerang	Displays boomerang information on the DRP agent.
ttl ip	Configures the IP TTL value for the boomerang response packets sent from the boomerang client to the DNS client in number of hops.

ttl ip

To configure the IP time-to-live (TTL) value for the boomerang response packets sent from the boomerang client to the DNS client, use the **ttl ip** command in boomerang configuration mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

ttl ip *hops*

no ttl ip *hops*

Syntax Description

hops	Number of hops that occur between the boomerang client and the DNS client before the boomerang response packet fails. Range is from 1 to 255.

Defaults

No default behavior or values.

Command Modes

Boomerang configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

The **ttl ip** command can be used only on a Director Response Protocol (DRP) agent. The boomerang client is the DRP agent.

The **ttl ip** command configures the maximum number of hops allowed between the boomerang client and the DNS client, after which the boomerang response packet fails. If the user wants to restrict the contending proxies only to nearby ones, the value of the **ttl ip** command can be set to a specific number within the allowed range. Any proxy outside of this range will be automatically disqualified in the boomerang race because its replies will never reach the DNS client. Because the **ttl ip** command specifies the number of hops for which a response from a client will live, it allows faraway proxies to avoid wasting bandwidth.

Examples

In the following example, the number of hops that occur between the boomerang client and the DNS client before the boomerang response packet fails is configured as 2:

```
Router(config)# ip drp domain www.boom1.com
Router(config-boomerang)# ttl ip 2

Router# show running-config
.
.
.
ip drp domain www.boom1.com
ip-ttl 2
```

Related Commands

Command	Description
alias (boomerang)	Configures an alias name for a specified domain.
ip drp domain	Adds a new domain to the DistributedDirector client or configures an existing domain and puts the client in boomerang configuration mode.
server (boomerang)	Configures the server address for a specified boomerang domain.
show ip drp	Displays DRP statistics on DistributedDirector or a DRP server agent.
show ip drp boomerang	Displays boomerang information on the DRP agent.
ttl dns	Configures the number of seconds for which an answer received from the boomerang client will be cached by the DNS client.

type dhcp

To configure a Dynamic Host Configuration Protocol Service Assurance Agent (SAA) operation, use the **type dhcp** command in SAA RTR configuration mode. To disable a DHCP SAA operation, use the **no** form of this command.

type dhcp [**source-ipaddr** *source-ip-address*] [**dest-ipaddr** *dest-ip-address*] [**option** *decimal-option* [**circuit-id** *circuit-id*] [**remote-id** *remote-id*] [**subnet-mask** *subnet-mask*]]

no type dhcp

Syntax Description

source-ipaddr *source-ip-address*	(Optional) Source name or IP address.
dest-ipaddr *dest-ip-address*	(Optional) Destination name or IP address.
option *decimal-option*	(Optional) Option number. The only currently valid value is 82. DHCP option 82 allows you to specify the circuit-id, remote-id, and/or the subnet-mask for the destination DHCP server.
circuit-id *circuit-id*	(Optional) Circuit ID in hexadecimal.
remote-id *remote-id*	(Optional) Remote ID in hexadecimal.
subnet-mask *subnet-mask*	(Optional) Subnet mask IP address. The default value is 255.255.255.0.

Defaults

No SAA operation type is associated with the operation number being configured.

Command Modes

SAA RTR configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.1(1)T	The following keywords were added: • **source-ipaddr** • **dest-ipaddr** • **option 82**

Usage Guidelines

You must configure the type of operation before you can configure any of the other characteristics of the operation.

If the source IP address is configured, then packets will be sent with that source address.

You may configure the **ip dhcp-server** command to identify the DHCP server that the DHCP operation will measure.

If the target IP address is configured, then only that device will be measured.

If the **ip dhcp-server** command is not configured and the target IP address is not configured, then DHCP discover packets will be sent on every available IP interface.

Option 82 is called the Relay Agent Information option and is inserted by the DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server. Servers recognizing the Relay Agent Information option may use the information to implement IP address or other parameter assignment policies. The DHCP Server echoes the option back verbatim to the relay agent in server-to-client replies, and the relay agent strips the option before forwarding the reply to the client.

The Relay Agent Information option is organized as a single DHCP option that contains one or more suboptions that convey information known by the relay agent. The initial sub-options are defined for a relay agent that is co-located in a public circuit access unit. These suboptions are as follows: a **circuit-id** for the incoming circuit, a **remote-id** which provides a trusted identifier for the remote high-speed modem, and a **subnet-mask** designation for the logical IP subnet from which the relay agent received the client DHCP packet.

If an odd number of characters are specified for the **circuit-id**, a zero will be added to the end of the string.

Examples

In the following example, SAA operation number 4 is configured as a DHCP operation enabled for DHCP server 172.16.20.3:

```
Router(config)# rtr 4
Router(config-rtr)# type dhcp option 82 circuit-id 10005A6F1234
Router(config-rtr)# exit
Router(config)# ip dhcp-server 172.16.20.3
```

Related Commands

Command	Description
ip dhcp-server	Specifies which DHCP servers to use on a network, and specifies the IP address of one or more DHCP servers available on the network.
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.

type dlsw

To configure a data-link switching (DLSw) Service Assurance Agent (SAA) operation, use the **type dlsw** command in SAA RTR configuration mode. To remove the type configuration for the operation, use the **no** form of this command.

type dlsw peer-ipaddr *ip-address*

no type dlsw peer-ipaddr *ip-address*

Syntax Description

peer-ipaddr	Peer destination.
ip-address	IP address.

Defaults

No SAA operation type is associated with the operation number being configured.

Command Modes

SAA RTR configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

In order to configure a DLSw operation, the DLSw feature must be configured on the local and target routers.

You must configure the type of operation before you can configure any of the other characteristics of the operation.

The default for the optional characteristic **request-data-size** for a DLSw SAA operation is 0 bytes.

The default for the optional characteristic **timeout** for a DLSw SAA operation is 30 seconds.

Examples

In the following example, SAA operation number 4 is configured as a DLSw operation enabled for remote peer IP address 172.21.27.11. The data size is 15 bytes.

```
Router(config)# rtr 4
Router(config-rtr)# type dlsw peer-ipaddr 172.21.27.11
Router(config-rtr)# request-data-size 15
```

Related Commands

Command	Description
request-data-size	Sets the protocol data size in the payload of the SAA operation's request packet.
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.
show dlsw peers	Displays DLSw peer information.

type dns

To configure a Domain Name System (DNS) Service Assurance Agent (SAA) operation, use the **type dns** command in SAA RTR configuration mode. To remove the type configuration for the operation, use the **no** form of this command.

type dns target-addr {*ip-address* | *hostname*} **name-server** *ip-address*

no type dns target-addr {*ip-address* | *hostname*} **name-server** *ip-address*

Syntax Description

target-addr {*ip-address* | *hostname*}	Target (destination) IP address or hostname.
name-server *ip-address*	IP address of the Domain Name Server.

Defaults

No SAA operation type is associated with the operation number being configured.

Command Modes

SAA RTR configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

You must configure the type of operation before you can configure any of the other characteristics of the operation.

Examples

In the following example, SAA operation 7 is created and configured as a DNS operation using the target IP address 172.20.2.132:

```
Router(config)# rtr 7
Router(config-rtr)# type dns target-addr lethe name-server 172.20.2.132
```

Related Commands

Command	Description
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.

type echo

To configure an Service Assurance Agent (SAA) end-to-end echo response time probe operation, use the **type echo** command in SAA RTR configuration mode. To remove the operation from the configuration, use the **no** form of this command.

type echo protocol *protocol-type target* [**source-ipaddr** *ip-address*]

no type echo protocol *protocol-type target* [**source-ipaddr** *ip-address*]

Syntax Description

protocol *protocol-type target*	Protocol used by the operation. The *protocol-type target* argument combination must take one of the following forms: • **ipIcmpEcho** {*ip-address* | *hostname*}—IP/ICMP Echo. Requires a destination IP address or IP host name. • **snaRUEcho** *sna-hostname*—SNA's SSCP Native Echo. Requires the host name defined for the SNA's PU connection to VTAM. • **snaLU0EchoAppl** *sna-hostname* [*sna-application*] [*sna-mode*]—SNA LU type 0 connection to Cisco's NSPECHO host application that requires the host name defined for the SNA's PU connection to VTAM. Optionally, specify the host application name (the default is NSPECHO) and SNA mode to access the application. • **snaLU2EchoAppl** *sna-hostname* [*sna-application*] [*sna-mode*]—SNA LU type 2 connection to Cisco's NSPECHO host application that requires the host name defined for the SNA's PU connection to VTAM. Optionally, specify the host application name (the default is NSPECHO) and SNA mode to access the application.
source-ipaddr *ipaddr*	(Optional) Specifies an IP address as the source for the operation.

Defaults

The default SNA host *sna-application* name for an SNA LU type echo is NSPEcho.
The default data size for a IP/ICMP echo operation is 28 bytes.

Command Modes

SAA RTR configuration

Command History

Release	Modification
11.2	This command was introduced.
12.0(5)T	The **source-ipaddr** *ip-address* keyword/argument combination was added to support the specification of an IP source for the operation.

Usage Guidelines

Support of echo to a protocol and pathEcho to a protocol is dependent on the protocol type and implementation. In general most protocols support echo and few protocols support pathEcho.

Note Keywords are not case sensitive and are shown in mixed case for readability only.

Prior to sending a operation packet to the responder, the SAA sends a control message to the Responder to enable the destination port.

The default for the optional characteristic **request-data-size** for a ipIcmpEcho operation is 28 bytes. This is the payload portion of the Icmp packet, which makes a 64 byte IP packet.

Examples

In the following example, operation 10 is created and configured as an echo probe using the IP/ICMP Echo protocol and the destination IP address 172.16.1.175:

```
Router(config)# rtr 10
Router(config-rtr)# type echo protocol ipIcmpEcho 172.16.1.175
```

Related Commands

Command	Description
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.
show rtr configuration	Displays configuration values for RTR operations.

type frame-relay

To measure response time, frame loss, or data corruption across a Frame Relay permanent virtual circuit (PVC) using the Service Assurance Agent (SAA), use the **type frame-relay** command in global configuration mode. To delete a preconfigured frame-relay operation, use the **no** form of this command.

type frame-relay interface *interface-id* **dlci** *dlci-number*

no type frame-relay interface *interface-id* **dlci** *dlci-number*

Syntax Description

interface *interface-id*	Specifies the Frame Relay interface from which the operation will be sent. The *interface-id* argument should consist of the interface type and identification number (for example, **serial 1/0**).
dlci *dlci-number*	Specifies the Frame Relay PVC subinterface link that is assigned to the interface.

Defaults

No SAA operation type is associated with the operation number being configured.

Command Modes

RTR Entry configuration mode

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

The SAA Responder must be enabled on the target router before this command is used. Use the **rtr responder type frame-relay all** global configuration command or the **rtr responder** global configuration command on the target router to enable the responder.

If the first measurement does not have the correct values for frames sent and frames lost, the Frame Relay monitoring operation cannot work properly. There need to be at least two successful measurements for the frames sent and frames lost to be correct.

If the encapsulation on the target interface is not Frame Relay (for example, if the encapsulation is changed), the Frame Relay operation will be removed automatically from the configuration.

Examples

In the following example, a Frame Relay monitoring operation is configured to be sent from serial interface 0/1 using DLCI subinterface 22:

```
Router(config)# rtr 1
Router(config-rtr)# type frame-Relay interface Serial0 dlci 22
```

Related Commands

Command	Description
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.

type ftp

To configure an FTP operation, use the **type ftp** command in SAA RTR configuration mode. To remove the type configuration for the operation, use the **no** form of this command.

type ftp operation get url *url* [**source-ipaddr** *source-ip-address*] [**mode** {**passive** | **active**}]

no type ftp operation get url *url* [**source-ipaddr** *source-ip-address*] [**mode** {**passive** | **active**}]

Syntax Description

operation get	Specifies an FTP GET operation. (Support for other FTP operation types may be added in future releases.)
url *url*	Location information for the file to retrieve.
source-ipaddr *source-ip-address*	(Optional) Source address of the operation.
mode	(Optional) Specifies the transfer mode, either active or passive.
passive	FTP passive transfer mode. This is the default.
active	FTP active transfer mode.

Defaults

No SAA operation type is associated with the operation number being configured.

Command Modes

SAA RTR configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

GET is the only valid operation value. The URL must be in one of the following formats:

- ftp://user:password@host/filename
- ftp://host/filename

If the user and password keywords are not specified, the defaults are anonymous and test, respectively.

Examples

In the following example, an FTP operation is configured. Joe is the user and Young is the password. zxq is the host and test is the file name.

```
Router(config)# rtr 3
Router(config-rtr)# type ftp operation get ftp://joe:young@zxq/test
```

Related Commands

Command	Description
show rtr collection-statistics	Displays statistical errors for all SAA operations or the specified operation.
show rtr operational-state	Displays the operational state of all SAA operations or the specified operation.

type http

To configure a Hypertext Transfer Protocol (HTTP) Service Assurance Agent (SAA) operation, use the **type http** command in SAA RTR configuration mode. To remove the type configuration for the operation, use the **no** form of this command.

type http operation {**get | raw**} **url** *url* [**name-server** *ip-address*] [**version** *version-number*] [**source-ipaddr** {*name* | *ip-address*}] [**source-port** *port-number*] [**cache** {**enable** | **disable**}] [**proxy** *proxy-url*]

no type http operation {**get | raw**} **url** *url* [**name-server** *ip-address*] [**version** *version-number*] [**source-ipaddr** {*name* | *ip-address*}] [**source-port** *port-number*] [**cache** {**enable** | **disable**}] [**proxy** *proxy-url*]

Syntax Description

operation get	Specifies an HTTP GET operation.
operation raw	Specifies an HTTP RAW operation.
url *url*	Specifies the URL of destination HTTP server.
name-server	(Optional) Specifies name of destination Domain Name Server.
ip-address	(Optional) IP address of Domain Name Server.
version	(Optional) Specifies version number.
version-number	(Optional) Version number.
source-ipaddr	(Optional) Specifies source name or IP address.
name	Source name.
ip-address	Source IP address.
source-port	(Optional) Specifies source port.
port-number	(Optional) Source port number.
cache	(Optional) Enables or disables download of cached HTTP page.
enable	Enables downloads of cached HTTP page.
disable	Disables download of cached HTTP page.
proxy	(Optional) Proxy information.
proxy-url	(Optional) Proxy information or URL.

Defaults

No SAA operation type is associated with the operation number being configured.

Command Modes

SAA RTR configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

You must configure the type of operation before you can configure any of the other characteristics of the operation.

Examples

HTTP GET operation

In this example operation 5 is created and configured as an HTTP GET operation. The destination URL is http://www.cisco.com.

```
Router(config)# rtr 5
Router(config-rtr)# type http operation get url http://www.cisco.com
Router(config-rtr)# exit
Router(config)# rtr schedule 5 start-time now
```

HTTP RAW operation using RAW submode

In this example operation 6 is created and configured as an HTTP RAW operation. To use the raw request commands, HTTP-RAW submode is entered using the **http-raw-request** command. The RTR HTTP-RAWsubmode is indicated by the (config-rtr-http) router prompt.

```
Router(config)# rtr 6
Router(config-rtr)# type http operation raw url http://www.cisco.com
Router(config-rtr)# http-raw-request
Router(config-rtr-http)# GET /index.html HTTP/1.0\r\n
Router(config-rtr-http)# \r\n
Router(config-rtr-http)# exit
Router(config)# rtr schedule 6 start-time now
```

HTTP RAW operation through a Proxy Server

In this example http://www.proxy.cisco.com is the proxy server and http://www.yahoo.com is the HTTP Server:

```
Router(config)# rtr 6
Router(config-rtr)# type http operation raw url http://www.proxy.cisco.com
Router(config-rtr)# http-raw-request
Router(config-rtr-http)# GET http://www.example.com HTTP/1.0\r\n
Router(config-rtr-http)# \r\n
Router(config-rtr-http)# exit
Router(config)# rtr schedule 6 start-time now
```

Related Commands

Command	Description
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.

type jitter

To configure a jitter Service Assurance Agent (SAA) operation, use the **type jitter** command in SAA RTR configuration mode. To disable a jitter operation, use the **no** form of this command.

type jitter dest-ipaddr {*name* | *ip-address*} **dest-port** *port-number* [**source-ipaddr** {*name* | *ip-address*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] [**num-packets** *number-of-packets*] [**interval** *inter-packet-interval*]

no type jitter dest-ipaddr {*name* | *ip-address*} **dest-port** *port-number* [**source-ipaddr** {*name* | *ip-address*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] [**num-packets** *number-of-packets*] [**interval** *inter-packet-interval*]

Syntax Description

dest-ipaddr	Destination for the operation.
name	Destination IP host name.
ip-address	Destination IP address.
dest-port	Destination port.
port-number	Port number of the destination port.
source-ipaddr	(Optional) Source IP address.
name	IP host name.
ip-address	IP address.
source-port	(Optional) Source port.
port-number	Port number of the source.
control	(Optional) Combined with the **enable** or **disable** keyword, enables or disables sending a control message to the destination port.
enable	Enables the SAA to send a control message to the destination port prior to sending a probe packet. This is the default value.
disable	Disables sending of control messages to the responder prior to sending a probe packet.
num-packets *number-of-packets*	(Optional) Number of packets, as specified by the number argument. The default value is 10.
interval *inter-packet-interval*	(Optional) Interpacket interval in milliseconds. The default value of the *inter-packet-interval* argument is 20 ms.

Defaults

No SAA operation type is associated with the operation number being configured.

The default for the optional characteristic **request-data-size** for a SAA Jitter operation is 32 bytes of UDP data.

Command Modes

SAA RTR configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

The **type jitter** command configures a UDP Plus SAA operation. The UDP Plus operation is a superset of the UDP echo operation. In addition to measuring UDP round trip time, the UDP Plus operation measures per-direction packet-loss and jitter (inter-packet delay variance). Packet loss is a critical element in SLAs, and Jitter statistics are useful for analyzing traffic in a VoIP network.

You must enable the SAA RTR Responder on the target router (using the rtr responder command) before you can configure a Jitter operation. Prior to sending a operation packet to the responder, the SAA sends a control message to the SAA RTR Responder to enable the destination port.

You must configure the type of operation before you can configure any of the other characteristics of the operation.

Examples

In the following example, operation 6 is created and configured as a Jitter operation using the destination IP address 172.30.125.15, the destination port number 2000, 20 packets, and an interval of 20:

```
Router(config)# rtr 6
Router(config-rtr)# type jitter dest-ip 172.30.125.15 dest-port 2000 num-packets 20
interval 20
```

Related Commands

Command	Description
request-data-size	Sets the payload size for SAA operation requests.
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.

type pathEcho

To configure an Internet Protocol/Internet Control Message Protocol (IP/ICMP) Path Echo Service Assurance Agent (SAA) operation, use the **type pathEcho** command in SAA RTR configuration mode. To remove the operation from the configuration, use the **no** form of this command.

type pathEcho protocol ipIcmpEcho {*ip-address* | *ip-hostname*}

no type pathEcho protocol ipIcmpEcho {*ip-address* | *ip-hostname*}

Syntax Description

protocol ipIcmpEcho	Specifies an IP/ICMP Echo operation. This is currently the only protocol type supported for the SAA Path Echo operation.
ip-address	Specifies the IP address of the target device.
ip-hostname	Specifies the designated IP name of the target device.

Defaults

No SAA operation type is associated with the operation number being configured.

Command Modes

SAA RTR configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Keywords are not case sensitive and are shown in mixed case for readability only.

Examples

In the following example, SAA operation 10 is created and configured as pathEcho probe using the IP/ICMP Echo protocol and the destination IP address 172.16.1.175:

```
Router(config)# rtr 10
Router(config-rtr)# type pathEcho protocol ipIcmpEcho 172.16.1.175
```

Related Commands

Command	Description
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.
show rtr configuration	Displays configuration values for RTR operations (probes).

type pathJitter

To configure an Service Assurance Agent (SAA) Path Jitter monitoring operation, use the **type pathJitter** command in RTR Entry configuration mode. To remove an inactive Path Jitter entry from the RTR configuration, use the **no** form of this command.

type pathJitter dest-ipaddress *ip-address* [**source-ipaddress** *source-ip*] [**num-packets** *packet-number*] [**interval** *time-ms*] [**targetOnly**]

no type pathJitter dest-ipaddress *ip-address* [**source-ipaddress** *source-ip*] [**num-packets** *packet-number*] [**interval** *time-ms*] [**targetOnly**]

Syntax Description

dest-ipaddress *ip-address*	Specifies the destination (target) IP address or host name.
source-ipaddress *source-ip*	(Optional) Specifies the source IP address that will be used for the operational probe packets.
num-packets *packet-number*	(Optional) The number of packets to be transmitted in each operation. The default value is 10.
interval *time-ms*	(Optional) Time interval between packets (in milliseconds). The default value is 20 ms.
targetOnly	(Optional) Sends test packets to the destination only (path is not traced).

Defaults

No SAA operation type is associated with the operation number being configured.

Command Modes

SAA RTR configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

The Path Jitter SAA operation traces a specified IP path from the source to the destination and then sends a specified number of packets to each hop along the traced path. Optionally, the time interval between each test packet can be specified.

If the number of packets and the time interval are not specified, the path jitter operation will use the default values.

If the **targetOnly** keyword is not used, the path jitter operation will trace the "hop-by-hop" IP path from the source to the destination and send the specified number of test packets to each hop along the trace path, using the specified time interval between each test packet.

If the **targetOnly** keyword is used, the command will cause the pathJitter operation to send echos to the destination only (the path from the source to the destination is not traced).

Examples

The following example enables the Path Jitter operation to trace the IP path to the destination 172.69.1.129 and send ten test packets to each hop with an interval of 20 ms between each test packet:

```
Router# config terminal
Router(config)# rtr 1
Router(config-rtr)# type pathJitter dest-ipaddr 172.69.1.129
```

The following example enables the Path Jitter operation to send 50 test packets to 172.69.5.6 with an interval of 30 ms between each test packet:

```
Router# config terminal
Router(config)# rtr 2
Router(config-rtr)# type pathJitter 172.69.5.6 num-packets 50 interval 30 targetOnly
```

type slm controller

To configure a Service Assurance Agent (SAA) operation as an SLM interface operation, and to specify the interface that the operation should be run on, use the **type slm controller** command in SAA RTR configuration mode. To remove or replace a previously configured SAA operation, use the **no rtr** *operation-number* global configuration command.

type slm controller *controller-id*

Syntax Description

controller-id	The controller type and slot/port number. Valid controller types include **E1**, **E3**, **T1**, and **T3**.

Defaults

No SAA operation type is associated with the operation number being configured.

Command Modes

SAA RTR configuration

Command History

Release	Modification
12.2(15)T	This command was introduced for T3 and E3 controllers using ATM. This command replaces the **type t1-slm** command.
12.3(1)	Support for controllers configured for Frame Relay was added.

Usage Guidelines

This SAA RTR configuration command specifies that the operation is an SLM physical controller operation, which provides information about the data link layer connection, and specifies the controller that the operation should be run on.

Controllers that can be monitored using this operation include T1, E1, T3, and E3.

The specified controller should be configured for Frame Relay or ATM.

Examples

In the following example, SAA operation 1 is configured as an SLM controller operation:

```
Router> enable
Password:
Router# configure terminal
Enter configuration commands, one per line.
Router(config)# rtr slm frame-relay statistics
Router(config)# rtr 1
Router(config-rtr)# type slm controller T1 0
Router(config-rtr-slm-if)# enhanced-history interval 900 buckets 100
Router(config-rtr-slm-if)# exit
Router(config)# rtr schedule 1 start-time now life forever
Router(config)# end
Router#
Router# show rtr configuration 1 | include Type
Type of operation to perform: slm controller
Reaction Type: None
Router#
```

Related Commands

Command	Description
rtr	Allows configuration of SAA operations by entering SAA RTR configuration mode for the specified operation number.
show rtr enhanced-history collection-statistics	Displays data for all collected history buckets for the specified SAA operation, with data for each bucket shown individually.
show rtr enhanced-history distribution-statistics	Displays enhanced history data for all collected buckets in a summary table.
type slm interface	Specifies that the SAA operation is an SLM interface operation, and specifies the interface that the operation should be run on.

type slm frame-relay interface

To configure a Service Assurance Agent (SAA) operation as an Service Level Management (SLM) Frame Relay (FR) interface operation, and to specify the interface that the operation should be run on, use the **type slm frame-relay interface** command in SAA RTR configuration mode. To remove or replace a previously configured SAA operation, use the **no rtr** *operation-number* global configuration command.

type slm frame-relay interface *interface-type interface-number*

Syntax Description

interface-type interface-number	The interface type (**Serial**) and number. An intervening space is not required.

Defaults

No SAA operation type is associated with the operation number being configured.

Command Modes

SAA RTR configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

The SAA SLM FR interface operation provides Frame Relay link (Layer 2) layer data. The **type slm frame-relay interface** command specifies the operation type and the interface that the operation should be run on. The specified interface should be configured for Frame Relay.

Frame Relay interface link statistics are used to monitor the basic health of a Frame Relay interface. This information includes some traffic counters, assorted error counts, and some performance-related counters.

To view the gathered statistics, use the **show rtr enhanced-history distribution-statistics** command or the **show rtr enhanced-history collection-statistics** command. Statistics gathered with this operation can also be retrieved from external network monitoring applications via the CNS event gateway.

Examples

In the following example, SAA operation 2 is configured as an SLM Frame Relay Interface operation:

```
Router> enable
Password:
Router# configure terminal
Enter configuration commands, one per line.
Router(config)# rtr slm frame-relay statistics
Router(config)# rtr 2
Router(config-rtr)# type slm frame-relay interface Serial0:0
Router(config-rtr-slm-fr-if)# enhanced-history interval 900 buckets 100
Router(config-rtr-slm-fr-if)# exit
Router(config)# rtr schedule 2 start-time now life forever
Router(config)# end
Router#
Router# show rtr configuration 2 | include Type
```

```
Type of operation to perform: Slm Frame-relay Interface
Reaction Type: None
```

Related Commands

Command	Description
rtr	Allows configuration of SAA operations by entering SAA RTR configuration mode for the specified operation number.
show rtr enhanced-history collection-statistics	Displays data for all collected history buckets for the specified SAA operation, with data for each bucket shown individually.
show rtr enhanced-history distribution-statistics	Displays enhanced history data for all collected buckets in a summary table.

type slm frame-relay pvc interface

To configure an Service Assurance Agent (SAA) operation as an Service Level Management (SLM)Frame Relay (FR) Circuit operation, and specify the interface that the operation should be run on, use the **type slm frame-relay pvc interface** command in SAA RTR configuration mode. To remove or replace a previously configured SAA operation, use the **no rtr** *operation-number* global configuration command.

type slm frame-relay pvc interface *interface-type interface-number dlci-number*

Syntax Description

interface-type interface-number	The interface type (**Serial**) and number. An intervening space is not required.
dlci-number	Data link connection identifier (DLCI) of the permanent virtual circuit (PVC) to be monitored.

Defaults

No SAA operation type is associated with the operation number being configured.

Command Modes

SAA RTR configuration mode

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

This command specifies that the operation is an SAA SLM FR circuit operation, which provides data for the specified circuit. The specified interface should be configured with a permanent virtual circuit (PVC) connection.

The Frame Relay circuit statistics are used to monitor the basic health of a Frame Relay circuit. This information includes some traffic counters, assorted error counts, and some performance-related counters.

This command puts the CLI into SAA SLM FR Circuit configuration mode (config-rtr-slm-fr-dlci).

Examples

In the following example, SAA operation 3 is configured as an SLM Frame Relay Circuit (or PVC) operation:

```
Router> enable
Password:
Router# configure terminal
Enter configuration commands, one per line.
Router(config)# rtr slm frame-relay statistics
Router(config)# rtr 3
Router(config-rtr)# type slm frame-relay pvc interface Serial0:0 111
Router(config-rtr-slm-fr-dlci)# enhanced-history interval 900 buckets 100
Router(config-rtr-slm-fr-dlci)# exit
Router(config)# rtr schedule 3 start-time now life forever
Router(config)# end
```

```
Router#
Router# show rtr configuration 3 | include Type
Type of operation to perform: Slm Frame-relay Pvc
Reaction Type: None
```

Related Commands

Command	Description
rtr	Allows configuration of SAA operations by entering SAA RTR configuration mode for the specified operation number.
show rtr enhanced-history collection-statistics	Displays data for all collected history buckets for the specified SAA operation, with data for each bucket shown individually.
show rtr enhanced-history distribution-statistics	Displays enhanced history data for all collected buckets in a summary table.

type slm interface

To configure a Service Assurance Agent (SAA) operation as an Service Level Management (SLM) interface operation, and to specify the interface that the operation should be run on, use the **type slm interface** command in SAA RTR configuration mode. To remove or replace a previously configured SAA operation, use the **no rtr** *operation-number* global configuration command.

type slm interface *type number*

Syntax Description

type number	The interface type and number. Interface types include **Serial** and **FR-ATM**. Alternatively, an Inverse Multiplexing over ATM (IMA) group number can be specified.

Defaults

No default behavior or values.

Command Modes

SAA RTR configuration

Command History

Release	Modification
12.2(11)T	This command was introduced to support ATM SLM operations.
12.2(13)T	This command was updated to support T1 IMA (ATM) interfaces.
12.3(1)	This command was updated to support FR SLM operations (Serial interfaces).

Usage Guidelines

The **type slm interface** SAA RTR configuration command specifies that the operation is an SLM physical interface operation, which provides information about the data link layer connection. The specified interface should be configured for Frame Relay or ATM.

Interfaces that can be monitored using this operation include Serial or HSSI (high speed serial interface) for Frame Relay interfaces, and IMA for ATM interfaces. To specify an HSSI interface, use the **Serial** keyword as the *type*.

In order for this operation to work, either the **atm slm statistics** global configuration command or the **rtr slm frame-relay statistics** global configuration command must be enabled on the device.

This command puts the CLI into SAA SLM controller/interface configuration mode, in which you can configure optional characteristics for the operation. To view the available options, enter the **?** command at the (config-rtr-slm-if) prompt.

Examples

In the following example, SAA operation 1 is configured as an SLM interface operation for a Frame Relay interface:

```
Router> enable
Password:
Router# configure terminal
Enter configuration commands, one per line.
```

```
Router(config)# rtr slm frame-relay statistics
Router(config)# rtr 1
Router(config-rtr)# type slm interface Serial 0.1
Router(config-rtr-slm-if)# enhanced-history interval 900 buckets 100
Router(config-rtr-slm-if)# exit
Router(config)# rtr schedule 1 start-time now life forever
Router(config)# end
Router#
Router# show rtr configuration 1 | include Type
Type of operation to perform: slm interface
Reaction Type: None
Router#
```

Related Commands

Command	Description
rtr	Allows configuration of SAA operations by entering SAA RTR configuration mode for the specified operation number.
show rtr enhanced-history collection-statistics	Displays data for all collected history buckets for the specified SAA operation, with data for each bucket shown individually.
show rtr enhanced-history distribution-statistics	Displays enhanced history data for all collected buckets in a summary table.
type slm controller	Specifies that the SAA operation is an SLM controller operation, and specifies the controller that the operation should be run on.

type tcpConnect

To define a tcpConnect probe, use the **type tcpConnect** command in Service Assurance Agent (SAA) RTR configuration mode. To remove the type configuration for the probe, use the **no** form of this command.

type tcpConnect dest-ipaddr {*name* | *ip-address*} **dest-port** *port-number* [**source-ipaddr** {*name* | *ip-address*} **source-port** *port-number*] [**control** {**enable** | **disable**}]

no type tcpConnect dest-ipaddr {*name* | *ip-address*} **dest-port** *port-number*

Syntax Description

dest-ipaddr *name* | *ip-address*	Destination of tcpConnect probe. *name* indicates IP host name. *ip-address* indicates IP address.
dest-port *port-number*	Destination port number.
source-ipaddr *name* | *ip-address*	(Optional) Source IP host name or IP address.
source-port *port-number*	(Optional) Port number of the source. When a port number is not specified, SAA picks the best IP address (nearest to the target) and available User Datagram Protocol (UDP) port.
control	(Optional) Specifies that the SAA control protocol should be used when running this probe. The control protocol is required when the probe's target is a Cisco router that does not natively provide the service (TCP service in this case). Combined with the **enable** or **disable** keyword, enables or disables sending a control message to the destination port. The default is that the control protocol is enabled. When enabled, the SAA sends a control message to the SAA Responder (if available) to enable the destination port prior to sending a probe packet.
enable	Enables the SAA collector to send a control message to the destination port prior to sending a probe packet. This is the default.
disable	Disables the SAA from sending a control message to the target prior to sending a probe packet.

Defaults

No SAA operation type is associated with the operation number being configured.

Command Modes

SAA RTR configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

You must configure an SAA operation type before you can configure any of the other characteristics of the operation.

The Transmission Control Protocol (TCP) Connection operation is used to discover the time it takes to connect to the target device. This operation can be used to test virtual circuit availability or application availability. If the target is a Cisco router, then SA Agent makes a TCP connection to any port number specified by the user. If the destination is a non-Cisco IP host, then the user must specify a known target port number (for example, 21 for FTP, 23 for Telnet, or 80 for HTTP Server). This operation is useful in testing Telnet or HTTP connection times.

Examples

In the following example, SAA operation 11 is created and configured as a tcpConnect probe using the destination IP address 172.16.1.175, and the destination port 2400:

```
Router(config)# rtr 11
Router(config-rtr)# type tcpConnect dest-ipaddr 172.16.1.175 dest-port 2400
```

Related Commands

Command	Description
rtr	Specifies an SAA operation begins configuration for that operation.
show rtr configuration	Displays configuration values for SAA operations.

type udpEcho

To define a udpEcho probe, use the **type udpEcho** command in Service Assurance Agent (SAA) RTR configuration mode. To remove the type configuration for the probe, use the **no** form of this command.

type udpEcho dest-ipaddr {*name* | *ip-address*} **dest-port** *port-number* [**source-ipaddr** {*name* | *ip-address*} **source-port** *port-number*] [**control** {**enable** | **disable**}]

no type udpEcho dest-ipaddr {*name* | *ip-address*} **dest-port** *port-number*

Syntax Description

dest-ipaddr *name* | *ip-address*	Destination of the udpEcho probe. Use an IP host name or IP address.
dest-port *port-number*	Destination port number. The range of port numbers is from 1 to 65,535.
source-ipaddr *name* | *ip-address*	(Optional) Source IP host name or IP address.
source-port *port-number*	(Optional) Port number of the source. When a port number is not specified, SAA picks the best IP address (nearest to the target) and available User Datagram Protocol (UDP) port.
control	(Optional) Specifies that the SAA RTR control protocol should be used when running this probe. The control protocol is required when the probe's target is a Cisco router that does not natively provide the service (UDP service in this case). Combined with the **enable** or **disable** keyword, enables or disables sending of a control message to the destination port. The default is that the control protocol is enabled.
enable	Enables the SAA collector to send a control message to the destination port prior to sending a probe packet. This is the default.
disable	Disables the SAA from sending a control message to the responder prior to sending a probe packet.

Defaults

No SAA operation type is associated with the operation number being configured.

Command Modes

SAA RTR configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

You must configure an operation type before you can configure any of the other characteristics of the operation.

The source IP address and port number are optional. If they are not specified, SAA selects the IP address nearest to the target and an available UDP port.

Examples

In the following example, SAA operation 12 is created and configured as udpEcho probe using the destination IP address 172.16.1.175 and destination port 2400:

```
Router# configure terminal
Router(config)# rtr 12
Router(config-rtr)# type udpEcho dest-ipaddr 172.16.1.175 dest-port 2400
```

Related Commands

Command	Description
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.
show rtr configuration	Displays configuration values for SAA operations.

undelete

To recover a file marked "deleted" on a Class A Flash file system, use the **undelete** command in EXEC mode.

undelete *index* [*filesystem***:**]

Syntax Description

index	A number that indexes the file in the **dir** command output.
*filesystem***:**	(Optional) A file system containing the file to undelete, followed by a colon.

Defaults

The default file system is the one specified by the **cd** command.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced for Class A Flash File Systems (platforms include the Cisco 7500 series and Cisco 12000 series).

Usage Guidelines

For Class A Flash file systems, when you delete a file, the Cisco IOS software simply marks the file as deleted, but it does not erase the file. This command allows you to recover a "deleted" file on a specified Flash memory device. You must undelete a file by its index because you could have multiple deleted files with the same name. For example, the "deleted" list could contain multiple configuration files with the name router-config. You undelete by index to indicate which of the many router-config files from the list to undelete. Use the **dir** command to learn the index number of the file you want to undelete.

You cannot undelete a file if a valid (undeleted) file with the same name exists. Instead, you first delete the existing file and then undelete the file you want. For example, if you had an undeleted version of the router-config file and you wanted to use a previous, deleted version instead, you could not simply undelete the previous version by index. You would first delete the existing router-config file and then undelete the previous router-config file by index. You can delete and undelete a file up to 15 times.

On Class A Flash file systems, if you try to recover the configuration file pointed to by the CONFIG_FILE environment variable, the system prompts you to confirm recovery of the file. This prompt reminds you that the CONFIG_FILE environment variable points to an undeleted file. To permanently delete all files marked "deleted" on a Flash memory device, use the **squeeze** EXEC command.

For further information on Flash File System types (classes), see http://www.cisco.com/warp/public/63/pcmciamatrix.html.

Examples

The following example recovers the deleted file whose index number is 1 to the Flash memory card inserted in slot 0:

```
Router# undelete 1 slot0:
```

Related Commands

Command	Description
delete	Deletes a file on a Flash memory device.
dir	Displays a list of files on a file system.
squeeze	Permanently deletes Flash files by squeezing a Class A Flash file system.

upgrade rom-monitor file

To reload the Upgrade ROMmon image on a Cisco 7200 VXR or Cisco 7301 router, use the **upgrade rom-monitor file** command in Privileged EXEC mode.

For the Cisco 7200 VXR router using the NPE-G1, the syntax is:

upgrade rom-monitor file {**bootflash** [*file-path*] | **disk0** [*file-path*] **| disk1** [*file-path*] | **disk2** [*file-path*] | **flash** [*file-path*] | **ftp** [*file-path*] | **slot0** [*file-path*] | **slot1** [*file-path*] | **tftp** [*file-path*]}

For the Cisco 7301 router, the syntax is:

upgrade rom-monitor file {**flash** [*file-path*] | **ftp** [*file-path*] | **disk0** [*file-path*] | **tftp** [*file-path*]}

Syntax Description

file-path	Directory path name or filename where the Upgrade ROMmon image is located.
bootflash	Filename location of Upgrade ROMmon image in boot flash memory.
disk0	Disk 0 is only present on a Cisco 7200 VXR that has an I/O controller and is always present on the Cisco 7301 router. The filename location of the Upgrade ROMmon image in disk 0 of the router chassis.
disk1	Disk 1 is only present on a Cisco 7200 VXR that has an I/O controller. The filename location of the Upgrade ROMmon image in disk 1 of the router chassis.
disk2	Disk 2 is always present on a Cisco 7200 VXR. The filename location of the Upgrade ROMmon image in disk 2 of the router chassis.
flash	Filename location of Upgrade ROMmon image in Flash memory.
ftp	Filename location of the Upgrade ROMmon image using File Transfer Protocol (FTP).
slot0, slot1	Slot 0 and slot 1 are only present on a Cisco 7200 VXR that has an I/O controller. The filename location of the Upgrade ROMmon image in slot 0 and slot 1 of the router chassis.
tftp	Filename location of the Upgrade ROMmon image on the TFTP server.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(28)S	This command was introduced on the Cisco 7200 VXR router.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T and supported on the Cisco 7200 VXR router and Cisco 7301 router.
12.3(9)	This command was integrated into Cisco IOS Release 12.3(9) and supported on the Cisco 7200 VXR router and Cisco 7301 router.

Usage Guidelines

A Cisco 7200 VXR that has an I/O controller card installed has the following additional devices on its chassis: disk 0, disk 1, slot 0, and slot 1.

Examples

The following example of a Cisco 7200 VXR using an I/O controller loads the Upgrade ROMmon image from a disk 1 filename:

```
Router# upgrade rom-monitor file disk1:C7200_NPEG1_RMFUR.srec.123-4r.T1
This command will reload the router. Continue? [yes/no]:yes
ROMMON image upgrade in progress.

Erasing boot flash eeeeeeeeeeeeeeeeee
Programming boot flash pppppp
Now Reloading via hard watchdog timeout
```

The following example on a Cisco 7301 router loads the Upgrade ROMmon image from a specified TFTP file location:

```
Router# upgrade rom-monitor file tftp://00.0.00.0/biff/C7301_RMFUR.srec
Loading biff/C7301_RMFUR.srec from 00.0.00.0 (via GigabitEthernet0/1):
 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 392348 bytes]

This command will reload the router. Continue? [yes/no]:yes
ROMMON image upgrade in progress.
Erasing boot flash eeeeeeeeeeeeeeeeee
Programming boot flash ppppp
Now Reloading via hard watchdog timeout

Unexpected exception, CP
System Bootstrap, Version 12.2(20031011:151758) [biff]
Copyright (c) 2004 by cisco Systems, Inc.

 Running new upgrade for first time

System Bootstrap, Version 12.2(20031011:151758) [biff]
Copyright (c) 2004 by cisco Systems, Inc.

ROM:Rebooted by watchdog hard reset
C7301 platform with 1048576 Kbytes of main memory


Upgrade ROMMON initialized
rommon 1 >
```

upgrade rom-monitor preference

To select a ReadOnly or Upgrade ROMmon image to be booted on the next reload of a Cisco 7200 VXR or Cisco 7301router, use the **upgrade rom-monitor preference** command in privileged EXEC mode.

upgrade rom-monitor preference [**readonly** | **upgrade**]

Syntax Description

readonly	Selects the ReadOnly ROMmon image to be booted on the next reload.
upgrade	Selects the Upgrade second ROMmon image to be booted on the next reload.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(28)S	This command was introduced on the Cisco 7200 VXR router.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T and supported on the Cisco 7200 VXR router and Cisco 7301 router.
12.3(9)	This command was integrated into Cisco IOS Release 12.3(9) and supported on the Cisco 7200 VXR router and Cisco 7301 router.

Usage Guidelines

After running the **upgrade rom-monitor preference** command, you must reload the router for the selected ROMmon image to take effect.

Use the **rommon-pref** command when you are in ROMmon mode.

Examples

The following example applicable to both the Cisco 7200 VXR and Cisco 7301 routers selects the ReadOnly ROMmon image to be booted on the next reload of the router:

```
Router# upgrade rom-monitor preference readonly
You are about to mark ReadOnly region of ROMMON for the highest boot preference.
Proceed? [confirm]
Done! Router must be reloaded for this to take effect.
```

Related Commands

Command	Description
rommon-pref	Selects a ReadOnly or Upgrade ROMmon image to be booted on the next reload when you are in ROMmon mode.

vacant-message

To display an idle terminal message, use the **vacant-message** command in line configuration mode. To remove the default vacant message or any other vacant message that may have been set, use the **no** form of this command.

vacant-message [*d message d*]

no vacant-message

Syntax Description

d	(Optional) Delimiting character that marks the beginning and end of the vacant-message. Text delimiters are characters that do not ordinarily appear within the text of a title, such as slash (/), double quote ("), or tilde (~). ^C is reserved for special use and should not be used in the message.
message	(Optional) Vacant terminal message.

Defaults

The format of the default vacant message is as follows:

```
<blank lines>
hostname tty# is now available
<blank lines>
Press RETURN to get started.
```

This message is generated by the system.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command enables the banner to be displayed on the screen of an idle terminal. The **vacant-message** command without any arguments restores the default message.

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

Note For a rotary group, you need to define only the message for the first line in the group.

Examples

The following example turns on the system banner and displays this message:

```
line 0
vacant-message #
                Welcome to Cisco Systems, Inc.
                 Press Return to get started.
```

verify

To verify the checksum of a file on a Flash memory file system, use the **verify** command in EXEC mode.

verify [**/md5** [*md5-value*]] *filesystem***:**[*file-url*]

Syntax Description

/md5	(Optional) Calculates and displays the MD5 value for the specified software image. Compare this value with the value available on Cisco.com for this image.
md5-value	(Optional) The known MD5 value for the specified image. When an MD5 value is specified in the command, the system will calculate the MD5 value for the specified image and display a message verifying that the MD5 values match or that there is a mismatch.
*filesystem***:**	(Optional) File system or directory containing the files to list, followed by a colon. Standard file system keywords for this command are **flash:** and **bootflash:**.
file-url	(Optional) The name of the files to display on a specified device. The files can be of any type. You can use wildcards in the filename. A wildcard character (*) matches all patterns. Strings after a wildcard are ignored.

Defaults

The current working device is the default device (file system).

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(4)T	The **/md5** keyword was added.

Usage Guidelines

This command replaces the **copy verify** and **copy verify flash** commands.

Use the **verify** command to verify the checksum of a file before using it.

Each software image that is distributed on disk uses a single checksum for the entire image. This checksum is displayed only when the image is copied into Flash memory; it is not displayed when the image file is copied from one disk to another.

Before loading or duplicating a new image, record the checksum and MD5 information for the image so that you can verify the checksum when you copy the image into Flash memory or onto a server. A variety of image information is available on Cisco.com. For example, you can get the Release, Feature Set, Size, BSD Checksum, Router Checksum, MD5, and Publication Date information by clicking on the image file name prior to downloading it from the Software Center on Cisco.com.

To display the contents of Flash memory, use the **show flash** command. The Flash contents listing does not include the checksum of individual files. To recompute and verify the image checksum after the image has been copied into Flash memory, use the **verify** command. Note, however, that the **verify**

command only performs a check on the integrity of the file after it has been saved in the file system. It is possible for a corrupt image to be transferred to the router and saved in the file system without detection. If a corrupt image is transferred successfully to the router, the software will be unable to tell that the image is corrupted and the file will verify successfully.

To use the message-digest5 (MD5) hash algorithm to ensure file validation, use the **verify** command with the **/md5** option. MD5 is an algorithm (defined in RFC 1321) that is used to verify data integrity through the creation of a unique 128-bit message digest. The **/md5** option of the **verify** command allows you to check the integrity of a Cisco IOS software image by comparing its MD5 checksum value against a known MD5 checksum value for the image. MD5 values are now made available on Cisco.com for all Cisco IOS software images for comparison against local system image values.

To perform the MD5 integrity check, execute the **verify** command using the **/md5** keyword. For example, executing the **verify flash:c7200-is-mz.122-2.T.bin /md5** command will calculate and display the MD5 value for the software image. Compare this value with the value available on Cisco.com for this image.

Alternatively, you can get the MD5 value from Cisco.com first, then specify this value in the command syntax. For example, executing the **verify flash:c7200-is-mz.122-2.T.bin /md5 8b5f3062c4caeccae72571440e962233** command will display a message verifying that the MD5 values match or that there is a mismatch. A mismatch in MD5 values means that either the image is corrupt or the wrong MD5 value was entered.

Examples

In the following example, the **verify** command is used to check the integrity of the file c7200-js-mz on the Flash memory card inserted in slot 0:

```
Router# dir slot0:

Directory of slot0:/

  1  -rw-     4720148   Aug 29 1997 17:49:36  hampton/nitro/c7200-j-mz
  2  -rw-     4767328   Oct 01 1997 18:42:53  c7200-js-mz
  5  -rw-         639   Oct 02 1997 12:09:32  rally
  7  -rw-         639   Oct 02 1997 12:37:13  the_time

20578304 bytes total (3104544 bytes free)
Router# verify slot0:c7200-js-mz
Verified slot0:c7200-js-mz
```

In the following example, the **/md5** keyword is used to display the MD5 value for the image:

```
Router# verify /md5 disk1:
Verify filename []? c7200-js-mz
.................................
.................................
.................................
.................................
.................................
.............................Done!
verify /md5 (disk1:c7200-js-mz) = 0f369ed9e98756f179d4f29d6e7755d3
```

In the following example, the known MD5 value for the image (obtained from Cisco.com) is specified in the **verify** command, and the system checks the value against the stored value:

```
Router# verify /md5 disk1:c7200-js-mz ?
  WORD  Expected md5 signature
  <cr>
router# verify /md5 disk1:c7200-js-mz 0f369ed9e98756f179d4f29d6e7755d3
.................................
.................................
```

```
................................
................................
................................
.............................Done!
Verified (disk1:c7200-js-mz) = 0f369ed9e98756f179d4f29d6e7755d3
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
copy	Copies any file from a source to a destination.
dir	Displays a list of files on a file system.
pwd	Displays the current setting of the **cd** command.
show file systems	Lists available file systems.

verify-data

To cause the Service Assurance Agent (SAA) operation to check each response for corruption, use the **verify-data** command in SAA RTR configuration mode. To return to the default value, use the **no** form of this command.

verify-data

no verify-data

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

SAA RTR configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Only use the **verify-data** command when corruption may be an issue.

Caution Do not enable this feature during normal operation because it causes unnecessary overhead.

Examples

In the following example, operation 5 is configured to verify the data for each response:

```
Router(config)# rtr 5
Router(config-rtr)# type echo protocol ipIcmpEcho 172.16.1.174
Router(config-rtr)# response-data-size 2
Router(config-rtr)# verify-data
```

Related Commands

Command	Description
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.

vrf (SAA)

To allow monitoring within Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) using Service Assurance Agent (SAA) operations, use the **vrf** command in RTR Entry configuration mode.

vrf *vrf-name*

Syntax Description

vrf-name	Name of the VRF.

Defaults

No default behavior or values.

Command Modes

SAA (RTR Entry) configuration mode

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

If the **vrf** command is configured for an SAA operation, the SAA uses *vrf-name* to identify the VRF for this operation. This command should only be used if it is necessary to measure the response time over the VPN tunnel.

Examples

The following examples illustrate how to set up different SAA operations that support MPLS VPNs. These examples show how test traffic can be sent in an already existing VPN tunnel between two endpoints. Only the following operations can measure response time of a VPN tunnel.

Note that for all of the following operation types, the source IP address is not specified. The SAA will automatically specify the correct source interface when the **vrfName** command is used.

Configuring an Echo Operation Example

```
rtr 1
   type echo protocol ipIcmpEcho 1.1.1.1
   vrf vpn1
  end
rtr schedule 1 start now

Configuring a Path Echo Operation Example

rtr 1
  type pathEcho protocol ipIcmpEcho 1.1.1.1
  vrfName vpn1
rtr schedule 1 start now


Configuring a UDP Echo Operation Example

rtr 1
```

```
  type udpEcho dest-ipaddr 1.1.1.1 dest-port 1213
  vrf vpn1
rtr schedule 1 start now

Configuring a Jitter Operation Example

rtr 1
  type jitter dest-ipaddr 1.1.1.1 dest-port 1213
  vrf vpn1
rtr schedule 1 start now
```

Related Commands

Command	Description
type echo	Configures an SAA Echo operation.

where

To list the open sessions, use the **where** command in EXEC mode.

where

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced in a release prior to Cisco IOS Release 10.0.

Usage Guidelines

The **where** command displays all open sessions associated with the current terminal line.

The break (Ctrl-Shift-6, x), **where**, and **resume** commands are available with all supported connection protocols.

Examples

The following is sample output from the **where** command:

```
Router# where
Conn Host                 Address          Byte    Idle  Conn Name
   1 MATHOM               192.31.7.21         0       0  MATHOM
*  2 CHAFF                131.108.12.19       0       0  CHAFF
```

The asterisk (*) indicates the current terminal session.

Table 136 describes the fields shown in the display.

Table 136 where Field Descriptions

Field	Description
Conn	Name or address of the remote host to which the connection is made.
Host	Remote host to which the router is connected through a Telnet session.
Address	IP address of the remote host.
Byte	Number of unread bytes for the user to see on the connection.
Idle	Interval (in minutes) since data was last sent on the line.
Conn Name	Assigned name of the connection.

Related Commands

Command	Description
show line	Displays information about all lines on the system or the specified line.
show sessions	Displays information about open LAT, Telnet, or rlogin connections.

width

To set the terminal screen width, use the **width** command in line configuration mode. To return to the default screen width, use the **no** form of this command.

width *characters*

no width

Syntax Description

characters	Number of character columns displayed on the terminal. The default is 80 characters.

Defaults

80 character columns

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

By default, the route provides a screen display width of 80 characters. You can reset this value for the current session if it does not meet the needs of your terminal.

The rlogin protocol uses the value of the *characters* argument to set up terminal parameters on a remote host.

Examples

In the following example the location for line 7 is defined as "console terminal" and the display is set to 132 columns wide:

```
Router(config)# line 7
Router(config-line)# location console terminal
Router(config-line)# width 132
```

Related Commands

Command	Description
terminal width	Sets the number of character columns on the terminal screen for the current session.

write core

To test the configuration of a core dump setup, use the **write core** command in privileged EXEC mode.

write core [*hostname* [**LINE**] | *destination-address* [**LINE**]]

Syntax Description

hostname	(Optional) Host name of the remote server where the core dump file is to be written.
destination-address	(Optional) IP address of the remote server where the core dump file is to be written.
LINE	(Optional) Assigns the name "LINE" to the core dump file.

Defaults

If the *hostname* or *destination* arguments are not specified, the core dump file is written to the IP address or hostname specified by the **exception dump** command.

If the **LINE** keyword is not specified, the name of the core dump file is assigned as the host name of the remote server followed by the word "-core."

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

When a router reloads, it is sometimes useful to obtain a full copy of the memory image (called a core dump) to identify the cause of the reload. Core dumps are generally useful to your technical support representative. Not all types of router reloads will produce a core dump.

The **write core** command causes the router to generate a core dump without reloading, which may be useful if the router is malfunctioning but has not reloaded. The core dump files will be the size of the respective memory regions. It is important to remember that the entire memory region is dumped, not just the memory that is in use.

Caution Use the **write core** command only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. When using this command, the router will not reload until the content of its memory is dumped. This event might take some time, depending on the amount of DRAM present on the router. Also, the resulting binary file, which is very large, must be transferred to a Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP), or remote copy protocol (rcp) server and subsequently interpreted by technical personnel who have access to source code and detailed memory maps.

Depending on your TFTP server, you might need to create an empty target file to which the router can write the core dump.

Examples

The following example shows how to test the configuration of a core dump setup. In this example, the core dump file is written to the remote server with the host name test.

```
write core test
```

write erase

The **write erase** command is replaced by the **erase nvram:** command. See the description of the **erase** command for more information.

write memory

The **write memory** command has been replaced by the **copy system:running-config nvram:startup-config** command. See the description of the **copy** command for more information.

write mib-data

To save MIB Persistence configuration data to NVRAM, use the **write mib-data** command in EXEC mode.

write mib-data

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

Any modified MIB data must be written to NVRAM memory using the **write mib-data** command. If the **write mib-data** command is not used, modified MIB data is not saved automatically.

Examples

The following example enables Event MIB Persistence and writes MIB data to NVRAM:

```
Router(config)# snmp mib persist event
Router(config)# end
Router# write mib-data
```

Related Commands

Command	Description
snmp mib persist	Enables MIB persistence.

write network

The **write network** command is replaced by the **copy system:running-config** *destination-url*. See the description of the **copy** command for more information.

write terminal

The **more system:running-config** command is replaced by the **write terminal** command. See the description of the **more** command for additional information.

xmodem

To copy a Cisco IOS image to a router using the ROM monitor and the Xmodem or Ymodem protocol, use the **xmodem** command in ROM monitor mode.

xmodem [**-c**] [**-y**] [**-e**] [**-f**] [**-r**] [**-x**] [**-s** *data-rate*] [*filename*]

Syntax Description

-c	(Optional) CRC-16 checksumming, which is more sophisticated and thorough than standard checksumming.
-y	(Optional) Uses the Ymodem protocol for higher throughput.
-e	(Optional) Erases the first partition in Flash memory before starting the download. This option is only valid for the Cisco 1600 series.
-f	(Optional) Erases all of Flash memory before starting the download. This option is only valid for the Cisco 1600 series.
-r	(Optional) Downloads the file to DRAM. The default is Flash memory.
-x	(Optional) Do not execute Cisco IOS image on completion of the download.
-s *data-rate*	(Optional) Sets the console port's data rate during file transfer. Values are **1200**, **2400**, **4800**, **9600**, **19200**, **38400**, and **115200 bps**. The default rate is specified in the configuration register. This option is only valid for the Cisco 1600 series.
filename	(Optional) Filename to copy. This argument is ignored when the **-r** keyword is specified, because only one file can be copied to DRAM. On the Cisco 1600 series routers, files are loaded to the ROM for execution.

Defaults

Xmodem protocol with 8-bit CRC, file downloaded into Flash memory and executed on completion.

Command Modes

ROM monitor

Command History

Release	Modification
11.2 P	This command was introduced.

Usage Guidelines

The Cisco 3600 series routers does not support XBOOT functionality. If your Cisco IOS image is erased or damaged, you cannot load a new image over the network.

Use the **xmodem** ROM monitor command to download a new system image to your router from a local personal computer (such as a PC, Mac, or UNIX workstation), or a remote computer over a modem connection, to the router's console port. The computer must have a terminal emulation application that supports these protocols.

Cisco 3600 Series Routers

Your router must have enough DRAM to hold the file being transferred, even if you are copying to Flash memory. The image is copied to the first file in internal Flash memory. Any existing files in Flash memory are erased. There is no support for partitions or copying as a second file.

Cisco 1600 Series Routers

If you include the **-r** option, your router must have enough DRAM to hold the file being transferred. To run from Flash, an image must be positioned as the first file in Flash memory. If you are copying a new image to boot from Flash, erase all existing files first.

Caution A modem connection from the telephone network to your console port introduces security issues that you should consider before enabling the connection. For example, remote users can dial in to your modem and access the router's configuration settings.

Note If the file to be downloaded is not a valid router image, the copy operation is automatically terminated.

Examples

The following example uses the **xmodem -c** *filename* ROM monitor command to copy the file named new-ios-image from a remote or local computer:

```
rommon > xmodem -c new-ios-image

Do not start the sending program yet...
         File size           Checksum   File name
   1738244 bytes (0x1a8604)   0xdd25 george-admin/c3600-i-mz

WARNING: All existing data in bootflash will be lost!
Invoke this application only for disaster recovery.
Do you wish to continue? y/n  [n]:  yes
Ready to receive file new-ios-image ...
```

Related Commands

Command	Description
copy xmodem:	Copies a Cisco IOS image from a local or remote computer (such as a PC, Macintosh, or UNIX workstation) to Flash memory on a Cisco 3600 series router using the Xmodem protocol.
copy ymodem:	Copies a Cisco IOS image from a local or remote computer (such as a PC, Macintosh, or UNIX workstation) to Flash memory on a Cisco 3600 series router using the Ymodem protocol.

xsm

To enable XML Subscription Manager (XSM) client access to the device, use the **xsm** command in global configuration mode. To disable XSM client access to the device, use the **no** form of this command.

xsm

no xsm

Syntax Description

This command has no arguments or keywords.

Defaults

XSM client access to the device is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

This command requires that the **ip http server** command is enabled. Enabling the **xsm** command also enables the **xsm vdm** and **xsm edm** commands. This command must be enabled for the XSM client (such as VPN Device Manager [VDM]) to operate.

Examples

In the following example, access by remote XSM clients to XSM data on the device is disabled:

```
Router# no xsm
```

Related Commands

Command	Description
ip http server	Enables a device to be reconfigured through the Cisco browser interface.
show xsm status	Displays information and status about clients subscribed to the XSM server.
show xsm xrd-list	Displays all XRDs for clients subscribed to the XSM server.
xsm dvdm	Grants access to switch operations.
xsm edm	Grants access to EDM monitoring and configuration data.
xsm vdm	Grants access to VPN-specific monitoring and configuration data.

xsm dvdm

To enable switch-specific configuration data (for example, configuring switch ports and VLANs) when running VPN Device Manager (VDM) on a switch, use the **xsm dvdm** command in global configuration mode. To disable switch-specific configuration data for VDM, use the **no** form of this command.

xsm dvdm

no xsm dvdm

Syntax Description

This command has no arguments or keywords.

Defaults

Access to switch-specific configuration data is enabled when XSM is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(9)YO1	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Access to switch-specific configuration data (dVDM) is enabled by default when XSM is enabled.

The **no xsm dvdm** command allows you to disable only switch-specific XSM data. Note however that disabling dVDM will prevent the VDM application from communicating properly with the device (switch). There is minimal performance impact associated with leaving dVDM enabled.

Examples

In the following example, access to switch-specific configuration data is disabled in XSM:

```
Router(config)# no xsm dvdm
```

Related Commands

Command	Description
xsm	Enables XSM client access to the router.
xsm edm	Grants access to EDM monitoring and configuration data.
xsm history vdm	Enables specific VPN statistics collection on the XSM server.
xsm vdm	Grants access to VPN-specific monitoring and configuration data.

xsm edm

To grant access to Embedded Device Manager (EDM) monitoring and configuration data, use the **xsm edm** command in global configuration mode. To cancel access to EDM monitoring and configuration data, use the **no** form of this command.

xsm edm

no xsm edm

Syntax Description

This command has no arguments or keywords.

Defaults

Access to EDM monitoring and configuration data is granted by default if XSM is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

This command exists to allow you to disable EDM using the **no xsm edm** form of the command. EDM is enabled by default when XSM is enabled.

EDM provides the following generic information to the VPN Device Manager (VDM):

- Relevant interfaces
- IP routing
- Access-list details
- Basic device health

Note that disabling EDM prevents XSM clients (such as VDM) from working properly and also disables the **xsm history edm** command. There is minimal performance impact associated with leaving EDM enabled.

Examples

In the following example, access to EDM data is disabled:

```
Router(config)# xsm
Router(config)# no xsm edm
```

Related Commands

Command	Description
xsm	Enables XSM client access to the router.
xsm dvdm	Grants access to switch operations.
xsm history edm	Enables statistics collection for the EDM on the XSM server.
xsm vdm	Grants access to VPN-specific monitoring and configuration data.

xsm history edm

To enable statistics collection for the Embedded Device Manager (EDM) on the XML Subscription Manager (XSM) server, use the **xsm history edm** command in global configuration mode. To disable statistics collection for the EDM on the XSM server, use the **no** form of this command.

xsm history edm

no xsm history edm

Syntax Description

This command has no arguments or keywords.

Defaults

EDM statistics collection is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use this command to save up to five days of data. Historical information on items such as RAM and CPU utilization is gathered and made available, thus enabling XSM clients (such as VPN Device Manager [VDM]) to display charts and data. Use of this command consumes resources on the device. Disabling this command clears all your historical data, as the XSM server does not save this data between reloads.

Examples

In the following example, statistics collection for the EDM is enabled on the XSM server:

```
Router(config)# xsm
Router(config)# xsm history edm
```

Related Commands

Command	Description
xsm	Enables XSM client access to the router.
xsm edm	Grants access to EDM monitoring and configuration data.
xsm history vdm	Enables specific VPN statistics collection on the XSM server.

xsm history vdm

To enable specific VPN statistics collection on the XML Subscription Manager (XSM) server, use the **xsm history vdm** command in global configuration mode. To disable collection of specific selected VPN statistics on the XSM server, use the **no** form of this command.

xsm history vdm

no xsm history vdm

Syntax Description

This command has no arguments or keywords.

Defaults

VPN statistics collecting is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

With this command enabled, you can save up to five days of data. Historical information on items such as the number of active IKE tunnels, IPSec tunnels, total crypto throughput, and total throughput is gathered and made available, thus enabling XSM clients (such as VPN Device Manager [VDM]) to display charts and data. Use of this command consumes resources on the device. Disabling this command clears all your historical data. The XSM server does not save history data across reloads.

Examples

The following example shows how to enable specific VPN statistics collection on the XSM server:

```
Router(config)# xsm
Router(config)# xsm history vdm
```

Related Commands

Command	Description
xsm	Enables XSM client access to the router.
xsm history edm	Enables statistics collection for the EDM on the XSM server.
xsm vdm	Grants access to VPN-specific monitoring and configuration data.

xsm privilege configuration level

To enable the XML Subscription Manager (XSM) configuration privilege level required to subscribe to XML Request Descriptors (XRDs), use the **xsm privilege configuration level** command in global configuration mode. To remove a previously configured XSM configuration privilege level, use the **no** form of this command.

xsm privilege configuration level *number*

no xsm privilege configuration level *number*

Syntax Description

number	Privilege level. Valid values are from 1 to 15. The default is 15.

Defaults

Level 15

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

The privilege level for the **xsm privilege configuration level** command must be greater than or equal to the privilege level for the **xsm privilege monitor level** command. For example, if the **xsm privilege configuration 7** command is enabled, you need a minimum privilege level of 7 to subscribe to configuration XRDs. The higher the number the higher the privilege level. Trying to set a conflicting range of privilege settings will force the Cisco device to display the following message:

```
Attempt to set monitor privilege greater than configuration. Privilege denied.
```

You can check the XSM privilege level settings by using the **show xsm status** command. Use the **show xsm xrd-list** command to check which privilege level is required for each XRD.

Note The initial login set by your system administrator determines whether you have the necessary IOS privilege level for actually configuring the Cisco router. Ask your system administrator for more information about privilege levels.

Examples

The following example shows how to set a configuration privilege level of 15, and a monitor privilege level of 11 for subscription to XRDs. Users with a privilege level below 11 are denied access.

```
xsm privilege configuration level 15
xsm privilege monitor level 11
```

Related Commands

Command	Description
privilege	Configures IOS privilege parameters.
xsm privilege monitor level	Enables monitor privilege level to subscribe to XRDs.

xsm privilege monitor level

To enable the XML Subscription Manager (XSM) monitoring privilege level required to subscribe to XML Request Descriptors (XRDs), use the **xsm privilege monitor level** command in global configuration mode. To remove a previously configured XSM monitoring privilege level, use the **no** form of this command.

xsm privilege monitor level *number*

no xsm privilege monitor level *number*

Syntax Description

number	Privilege level. Valid values are from 1 to 15. The default is 15.

Defaults

Level 1

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

The privilege level for the **xsm privilege monitor level** command must be less than or equal to the privilege level for the **xsm privilege configuration level** command. For example, if the **xsm privilege monitor 7** command is enabled, you need a minimum privilege level of 7 to subscribe to monitor XRDs. The higher the number the higher the privilege level. Trying to set a conflicting range of privilege settings will force the Cisco device to display the following message:

```
Attempt to set monitor privilege greater than configuration. Privilege denied.
```

You can check the XSM privilege level settings by using the **show xsm status** command. Use the **show xsm xrd-list** command to check which privilege level is required for each XRD.

Note The initial login set by your system administrator determines whether you have the necessary IOS privilege level for actually configuring the Cisco router. Ask your system administrator for more information about privilege levels.

Examples

The following example shows how to set a configuration privilege level of 15 and a monitor privilege level of 11 for subscription to XRDs. Users with a privilege level below 11 are denied access.

```
xsm privilege configuration level 15
xsm privilege monitor level 11
```

Related Commands

Command	Description
privilege	Configures IOS privilege parameters.
xsm privilege configuration level	Enables configuration privilege level to subscribe to XRDs.

xsm vdm

To grant access to VPN-specific monitoring and configuration data for the VPN Device Manager (VDM), use the **xsm vdm** command in global configuration mode. To cancel access to VPN-specific monitoring and configuration data for VDM, use the **no** form of this command.

xsm vdm

no xsm vdm

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled (Access to VPN-specific monitoring and configuration data for the VDM is granted when XSM is enabled.)

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

This command enables access to the following VPN-specific information:

- IPSec
- IKE
- Tunneling
- Encryption
- Keys and certificates

If XSM is enabled, this command is enabled by default. Access to VPN-specific monitoring and configuration data within XSM can be disabled by using the **no** form of the command. However, disabling this command will prevent VDM from working properly and will also disable the **xsm history vdm** command. Leaving this command enabled has minimal performance impact.

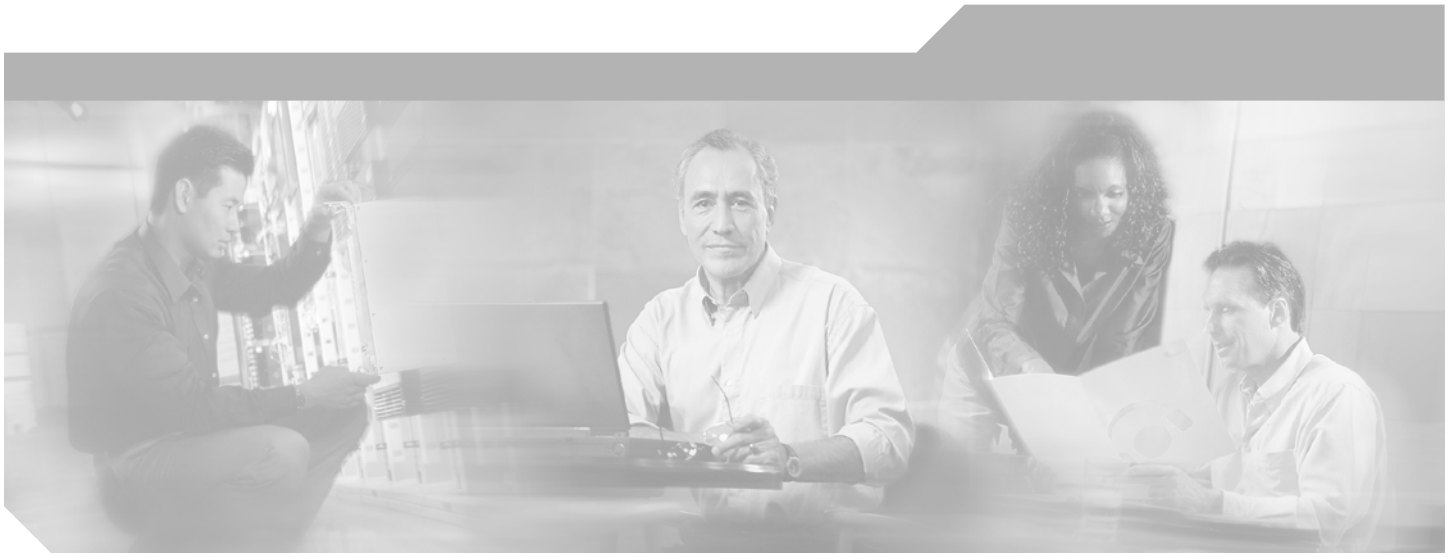
Examples

In the following example, access to VPN-specific monitoring and configuration data is disabled:

```
Router(config)# xsm
Router(config)# no xsm dvm
```

Related Commands

Command	Description
xsm	Enables XSM client access to the router.
xsm dvdm	Grants access to switch operations.
xsm edm	Grants access to EDM monitoring and configuration data.
xsm history vdm	Enables specific VPN statistics collection on the XSM server.



Appendix

ASCII Character Set and Hexidecimal Values

Some commands described in the Cisco IOS documentation set, such as the **escape-character** line configuration command, require that you enter the decimal representation of an ASCII character. Other commands, such as the **snmp-server group** command, make use of hexadecimal representations.

Table 137 provides code translations from the decimal numbers to their hexadecimal and ASCII equivalents. It also provides the keyword entry for each ASCII character. For example, the ASCII carriage return (CR) is decimal 13. Entering Ctrl-M at your terminal generates decimal 13, which is interpreted as a CR.

Table 137 ASCII Translation Table

Numeric Values		ASCII Character	Meaning	Keyboard Entry
Decimal	Hex			
0	00	NUL	Null	Ctrl-@
1	01	SOH	Start of heading	Ctrl-A
2	02	STX	Start of text	Ctrl-B
3	03	ETX	Break/end of text	Ctrl-C
4	04	EOT	End of transmission	Ctrl-D
5	05	ENQ	Enquiry	Ctrl-E
6	06	ACK	Positive acknowledgment	Ctrl-F
7	07	BEL	Bell	Ctrl-G
8	08	BS	Backspace	Ctrl-H
9	09	HT	Horizontal tab	Ctrl-I
10	0A	LF	Line feed	Ctrl-J
11	0B	VT	Vertical tab	Ctrl-K
12	0C	FF	Form feed	Ctrl-L
13	0D	CR	Carriage return (Equivalent to the Enter or Return key)	Ctrl-M
14	0E	SO	Shift out	Ctrl-N
15	0F	SI	Shift in/XON (resume output)	Ctrl-O
16	10	DLE	Data link escape	Ctrl-P

Table 137 ASCII Translation Table (continued)

Numeric Values		ASCII		
Decimal	Hex	Character	Meaning	Keyboard Entry
17	11	DC1	Device control character 1	Ctrl-Q
18	12	DC2	Device control character 2	Ctrl-R
19	13	DC3	Device control character 3	Ctrl-S
20	14	DC4	Device control character 4	Ctrl-T
21	15	NAK	Negative acknowledgment	Ctrl-U
22	16	SYN	Synchronous idle	Ctrl-V
23	17	ETB	End of transmission block	Ctrl-W
24	18	CAN	Cancel	Ctrl-X
25	19	EM	End of medium	Ctrl-Y
26	1A	SUB	Substitute/end of file	Ctrl-Z
27	1B	ESC	Escape	Ctrl-[
28	1C	FS	File separator	Ctrl-\
29	1D	GS	Group separator	Ctrl-]
30	1E	RS	Record separator	Ctrl-^
31	1F	US	Unit separator	Ctrl-_
32	20	SP	Space	Space
33	21	!	!	!
34	22	"	"	"
35	23	#	#	#
36	24	$	$	$
37	25	%	%	%
38	26	&	&	&
39	27	’	’	’
40	28	(	(	(
41	29	)	)	)
42	2A	*	*	*
43	2B	+	+	+
44	2C	,	,	,
45	2D	-	-	-
46	2E	.	.	.
47	2F	/	/	/
48	30	0	Zero	0
49	31	1	One	1
50	32	2	Two	2
51	33	3	Three	3

Table 137 ASCII Translation Table (continued)

Numeric Values		ASCII		
Decimal	Hex	Character	Meaning	Keyboard Entry
52	34	4	Four	4
53	35	5	Five	5
54	36	6	Six	6
55	37	7	Seven	7
56	38	8	Eight	8
57	39	9	Nine	9
58	3A	:	:	:
59	3B	;	;	;
60	3C	<	<	<
61	3D	=	=	=
62	3E	>	>	>
63	3F	?	?	?
64	40	@	@	@
65	41	A	A	A
66	42	B	B	B
67	43	C	C	C
68	44	D	D	D
69	45	E	E	E
70	46	F	F	F
71	47	G	G	G
72	48	H	H	H
73	49	I	I	I
74	4A	J	J	J
75	4B	K	K	K
76	4C	L	L	L
77	4D	M	M	M
78	4E	N	N	N
79	4F	O	O	O
80	50	P	P	P
81	51	Q	Q	Q
82	52	R	R	R
83	53	S	S	S
84	54	T	T	T
85	55	U	U	U
86	56	V	V	V

Table 137 ASCII Translation Table (continued)

Numeric Values		ASCII		
Decimal	Hex	Character	Meaning	Keyboard Entry
87	57	W	W	W
88	58	X	X	X
89	59	Y	Y	Y
90	5A	Z	Z	Z
91	5B	[	[	[
92	5C	\	\	\
93	5D	]	]	]
94	5E	^	^	^
95	5F	_	_	_
96	60	`	`	`
97	61	a	a	a
98	62	b	b	b
99	63	c	c	c
100	64	d	d	d
101	65	e	e	e
102	66	f	f	f
103	67	g	g	g
104	68	h	h	h
105	69	i	i	i
106	6A	j	j	j
107	6B	k	k	k
108	6C	l	l	l
109	6D	m	m	m
110	6E	n	n	n
111	6F	o	o	o
112	70	p	p	p
113	71	q	q	q
114	72	r	r	r
115	73	s	s	s
116	74	t	t	t
117	75	u	u	u
118	76	v	v	v
119	77	w	w	w
120	78	x	x	x
121	79	y	y	y

Table 137 ASCII Translation Table (continued)

Numeric Values		ASCII Character	Meaning	Keyboard Entry
Decimal	Hex			
122	7A	z	z	z
123	7B	{	{	{
124	7C	|	|	|
125	7D	}	}	}
126	7E	~	Tilde	~
127	7F	DEL	Delete	Del