

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.

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 | 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 preceded 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	<i>mode</i>	(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 user EXEC or privileged 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 <i>hex-address</i>	(Optional) Displays buffers at a specified address. Specify address in hexadecimal notation.
failures	(Optional) Displays buffer allocation failures.
pool <i>pool-name</i>	(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 <i>interface-type interface-number</i>	(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

User EXEC
Privileged 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.

Usage Guidelines

The peak field in the output of the **show buffers** command shows the maximum number of buffers created (highest total) and the time when that peak occurred relative to when you issued the **show buffers** command. Formats include weeks, days, hours, minutes, and seconds. Not all systems report a peak value, which means this field may not display in output.

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)
```

The following is sample output from the **show buffers** command with no arguments, showing only buffer pool information for Huge buffers. This output shows a highest total of five Huge buffers created five days and 18 hours before the command was issued.

```
Router> show buffers
```

```
Huge buffers, 18024 bytes (total 5, permanent 0, peak 5 @ 5d18h):
  4 in free list (3 min, 104 max allowed)
  0 hits, 1 misses, 101 trims, 106 created
  0 failures (0 no memory)
```

The following is sample output from the **show buffers** command with no arguments, showing only buffer pool information for Huge buffers. This output shows a highest total of 184 Huge buffers created one hour, one minute, and 15 seconds before the command was issued.

```
Router> show buffers
```

```
Huge buffers, 65280 bytes (total 4, permanent 2, peak 184 @ 01:01:15):
  4 in free list (0 min, 4 max allowed)
  32521 hits, 143636 misses, 14668 trims, 14670 created
  143554 failures (0 no memory)
```

The following is sample output from the **show buffers** command with an interface type and interface number:

```
Router> show buffers 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
```

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:	
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 18,024 bytes long.
total	Total number of this type of buffer.
permanent	Number of these buffers that are permanent.

Table 45 show buffers Field Descriptions (continued)

Field	Description
peak	Maximum number of buffers created (highest total) and the time when that peak occurred. Formats include weeks, days, hours, minutes, and seconds. Not all systems report a peak value, which means this field may not display in output.
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 <i>free list</i> to display 0.
failures	Total number of times a buffer creation failed. The failure may have occurred because of a number of different reasons, such as low processor memory, low IOMEM, or no buffers in the pool when called from interrupt context.
no memory	Number of times there has been low memory during buffer creation. Low or no memory during buffer creation may not necessarily mean that buffer creation failed; memory can be obtained from an alternate resource such as a fallback pool.

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.
<i>device-name</i>	Name of the neighbor about which you want information.
<i>device-name</i> *	You can enter an asterisk (*) at the end of an <i>entry-name</i> 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

<i>type</i>	(Optional) Type of interface about which you want information.
<i>number</i>	(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		
<i>type</i>	(Optional) Type of the interface connected to the neighbors about which you want information.	
<i>number</i>	(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	<i>name</i>	(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	<i>command</i>	Any Cisco IOS show command.
	 append url	<p>The addition of this syntax redirects the command output to the file location specified in the Universal Resource Locator (URL). The pipe () is required.</p> <p>The Cisco IOS File System (IFS) uses URLs to specify the location of a file system, directory, and file. Typical URL elements include:</p> <p><i>prefix:[directory]/filename</i></p> <p>Prefixes can be local file locations, such as flash: or disk0:. Alternatively, you can specify network locations using the following syntax:</p> <p>ftp:[[//[username[:password]@]location]/directory]/filename</p> <p>tftp:[[//location]/directory]/filename</p> <p>The rcp: prefix is not supported.</p>

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	<p>To display all URL prefixes that are supported for this command, use the show command append ? command.</p> <p>This command adds the show command output to the end of the specified file.</p>
-------------------------	---

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		
<i>command</i>		Any supported show command.
		A vertical bar (the “pipe” symbol) indicates that an output processing specification follows.
<i>regular-expression</i>		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 Ethernet** 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		
	<i>command</i>	Any supported show command.
		A vertical bar (the “pipe” symbol) indicates that an output processing specification follows.
	<i>regular-expression</i>	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

<i>command</i>	Any supported show command.
	A vertical bar (the “pipe” symbol) indicates that an output processing specification follows.
<i>regular-expression</i>	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 (is)** 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	<p>The addition of this syntax redirects the command output to the file location specified in the Universal Resource Locator (URL). The pipe () is required.</p> <p>The Cisco IOS File System (IFS) uses URLs to specify the location of a file system, directory, and file. Typical URL elements include:</p> <p><i>prefix:[directory]/filename</i></p> <p>Prefixes can be local file locations, such as flash: or disk0:. Alternatively, you can specify network locations using the following syntax:</p> <p>ftp:[[//[username[:password]@]location]/directory]/filename</p> <p>tftp:[[//location]/directory]/filename</p> <p>The rcp: prefix is not supported.</p>

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	<p>To display all URL prefixes that are supported for this command, use the show command redirect ? command.</p> <p>This command creates a new file at the specified location, or overwrites an existing file.</p>
------------------	---

Examples	<p>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:</p>
----------	--

```
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: <i>prefix:[directory]/filename</i> 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.