2

Internet Streamer CDS Release 2.4 Software Commands

This chapter contains an alphabetical listing of all the commands in Cisco Internet Streamer CDS Release 2.4 software. The Internet Streamer CDS software CLI is organized into the following command modes:

- EXEC mode—For setting, viewing, and testing system operations. It is divided into two access levels, user and privileged. To use the privileged access level, enter the **enable** command at the user access level prompt and then enter the privileged EXEC password when you see the password prompt.
- Global configuration mode—For setting, viewing, and testing the configuration of Internet Streamer CDS software features for the entire device. To use this mode, enter the **configure** command from privileged EXEC mode.
- Interface configuration mode—For setting, viewing, and testing the configuration of a specific interface. To use this mode, enter the **interface** command from global configuration mode.
- Other configuration modes—A number of configuration modes are available from the global configuration mode for managing specific features. The commands used to access these modes are marked with a footnote in Table 2-1.

See Chapter 1, "Using Command Modes," for a complete discussion of using CLI command modes.

Table 2-1 summarizes the Internet Streamer CDS commands and indicates the command mode for each command. The commands used to access configuration modes are marked with a footnote in Table 2-1. The same command may have different effects when entered in a different command mode, and for this reason, they are listed and documented separately. In Table 2-1, when the first occurrence is entered in EXEC mode, the second occurrence is entered in global configuration mode. When the first occurrence is entered in global configuration mode, the second occurrence is entered in interface configuration mode.

The Internet Streamer CDS software device mode determines whether the Internet Streamer CDS device is functioning as a Service Engine (SE), CDS Manager (CDSM), or Service Router (SR). The commands available from a specific CLI mode are determined by the Internet Streamer CDS device mode in effect. Table 2-1 also indicates the device mode for each command. *All* indicates that the command is available for every device mode.

Note When viewing this guide online, click the name of the command in the left column of the table to jump to the command page, which provides the command syntax, examples, and usage guidelines.

Note See Appendix A, "Acronyms" for an expansion of all acronyms used in this publication.

Table 2-1 CLI Commands

Command	Description	CLI Mode	Device Mode
access-lists	Configures the access control list entries.	Global configuration	SE
acquirer (EXEC)	Configures the content acquirer.	Privileged-level EXEC	SE
acquirer (global configuration)	Enables authentication when the acquirer obtains content through a proxy server.	Global configuration	SE
acquisition-distribution	Starts and stops the acquisition and distribution database cleanup process and the content acquisition and distribution process.	Privileged-level EXEC	SE
alarm overload-detect	Configures the detection of alarm overload.	Global configuration	All
asset	Configures the CISCO-ENTITY-ASSET-MIB.	Global configuration	All
authentication	Configures the authentication parameters.	Global configuration	All
authsvr	Enables and configures the Authorization server.	Global configuration	SE
bandwidth (global configuration)	Sets the allowable bandwidth usage and its duration for the Movie Streamer and WMT streaming media.	Global configuration	SE
bandwidth (interface configuration)	Sets the specified interface bandwidth to 10, 100, or 1000 Mbps.	Interface configuration	All
banner	Configures the EXEC, login, and message-of-the-day (MOTD) banners.	Global configuration	All
bitrate	Configures the maximum pacing bit rate for the Movie Streamer and configures WMT bit-rate settings.	Global configuration	SE
cache	Specifies the cache commands.	Global configuration	SE
capability	Modifies the capability configuration.	Global configuration	SE
cd	Changes the directory.	User-level EXEC & privileged-level EXEC	All
cdnfs	Manages the Internet Streamer CDS network file system (cdnfs).	Privileged-level EXEC	SE
cdsm	Configures the CDSM IP address and primary or standby role settings.	Global configuration	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.	Privileged-level EXEC	All
clock (exec)	Manages the system clock.	Privileged-level EXEC	All
clock (global configuration)	Sets the summer daylight saving time of day and time zone.	Global configuration	All
cms (EXEC)	Configures the Centralized Management System (CMS) embedded database parameters.	Privileged-level EXEC	All
cms (global configuration)	Schedules the maintenance and enables the Centralized Management System on a given node.	Global configuration	All
configure[1]	Enters configuration mode from privileged EXEC mode.	Privileged-level EXEC	All
copy	Copies the configuration or image files to and from the CD-ROM, flash memory, disk, or remote hosts.	Privileged-level EXEC	All
cpfile	Copies a file.	User-level EXEC & privileged-level EXEC	All
debug	Configures the debugging options.	Privileged-level EXEC	All
delfile	Deletes a file.	User-level EXEC & privileged-level EXEC	All
deltree	Deletes a directory and its subdirectories.	User-level EXEC & privileged-level EXEC	All
device	Configures the mode of operation on a device.	Global configuration	All
dir	Displays the files in a long list format.	User-level EXEC & privileged-level EXEC	All
direct-server-return	Enable a VIP for direct server return.	Global configuration	SE, SR
disable	Turns off the privileged EXEC commands.	Privileged-level EXEC	All
disk (EXEC)	Allocates the disks among the cdnfs and sysfs file systems.	Privileged-level EXEC	All
disk (global configuration)	Configures how the disk errors should be handled.	Global configuration	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
distribution	Reschedules and refreshes the content redistribution through multicast for all delivery services or a specified delivery service ID or name.	Privileged-level EXEC	SE, SR
dnslookup	Resolves a host or domain name to an IP address.	User-level EXEC & privileged-level EXEC	
enable[1]	Accesses the privileged EXEC commands.	User-level EXEC & privileged-level EXEC	All
end	Exits configuration and privileged EXEC modes.	Global configuration	All
exec-timeout	Configures the length of time that an inactive Telnet or Secure Shell (SSH) session remains open.	Global configuration	All
exit	Exits from interface, global configuration, or privileged EXEC modes.	All	All
external-ip	Configures up to a maximum of eight external IP addresses.	Global configuration	All
find-pattern	Searches for a particular pattern in a file.	Privileged-level EXEC	All
flash-media-streaming	Enables and configures Flash Media Streaming.	Global configuration	SE, SR
help	Obtains online help for the command-line interface.	Global configuration and user-level EXEC	All
hostname	Configures the device network name.	Global configuration	All
http	Configures the HTTP-related parameters.	Global configuration	SE, SR
icap	Enables the Internet Content Adaptation Protocol for supporting third-party software applications and plug-ins.	Global configuration	SE
icap service[1]	Configures ICAP service configurations. Provides access to the ICAP service configuration mode.	Global configuration	SE
install	Installs a new version of the caching application.	Privileged-level EXEC	All
interface[1]	Configures a Gigabit Ethernet or port-channel interface. Provides access to interface configuration mode.	Global configuration	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
ip	Configures the Internet Protocol.	Global configuration	All
ip access-list[1]	Creates and modifies the access lists for controlling access to interfaces or applications. Provides access to ACL configuration mode.	Global configuration	SE
ipv6	Specifies the default gateway's IPv6 address.	Global configuration	SE
kernel kdb	Enables the kernel debugger configuration mode.	Global configuration	All
line	Specifies the terminal line settings.	Global configuration	All
lls	Displays the files in a long list format.	User-level EXEC & privileged-level EXEC	All
logging	Configures system logging (syslog).	Global configuration	All
ls	Lists the files and subdirectories in a directory.	User-level EXEC & privileged-level EXEC	All
mkdir	Makes a directory.	User-level EXEC & privileged-level EXEC	All
mkfile	Makes a file (for testing).	User-level EXEC & privileged-level EXEC	All
movie-streamer	Enables and configures the Movie Streamer server.	Global configuration	SE
mtu	Sets the interface maximum transmission unit packet size.	interface configuration	All
no (global configuration)	Negates a global configuration command or sets its defaults.	Global configuration	All
no (interface configuration)	Negates an interface command or sets its defaults.	interface configuration	All
ntp	Configures the Network Time Protocol server.	Global configuration	All
ntpdate	Sets the NTP software clock.	Privileged-level EXEC	All
ping	Sends the echo packets.	User-level EXEC & privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
ping6	Pings the IPv6 address.	User-level EXEC & privileged-level EXEC	SE
port-channel	Configures the port-channel load-balancing options.	Global configuration	All
primary-interface	Configures a primary interface for the Internet Streamer CDS network to be a Gigabit Ethernet or port-channel interface.	Global configuration	All
pwd	Displays the present working directory.	User-level EXEC & privileged-level EXEC	All
qos	Globally enables QoS functionality on the device.	Global configuration	SE
radius-server	Configures the RADIUS authentication.	Global configuration	All
rcp	Enables RCP.	Global configuration	All
rea	Initiates the remote execution agent.	User-level EXEC & privileged-level EXEC	SE
reload	Halts a device and performs a cold restart.	Privileged-level EXEC	All
rename	Renames a file.	User-level EXEC & privileged-level EXEC	All
restore	Restores a device to its manufactured default status.	Privileged-level EXEC	All
rmdir	Removes a directory.	User-level EXEC & privileged-level EXEC	All
rtsp	Configures the Real-Time Streaming Protocol-related parameters.	Global configuration	SE
rule	Sets the rules by which the SE filters HTTP, HTTPS, and RTSP traffic.	Global configuration	SE
script	Checks the errors in a script or executes a script.	Privileged-level EXEC	All
service-router	Configures service routing.	Global configuration	SE, SR
setup	Configures the basic configuration settings and a set of commonly used caching services.	Privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
show	Displays the running system information.	User-level EXEC & privileged-level EXEC	All
show access-lists	Displays the access control list configuration.	User-level EXEC & privileged-level EXEC	SE
show acquirer	Displays the acquirer delivery service information and progress for a specified delivery service number or name.	User-level EXEC & privileged-level EXEC	SE
show alarms	Displays information on various types of alarms, their status, and history.	Privileged-level EXEC	All
show arp	Displays the Address Resolution Protocol entries.	User-level EXEC & privileged-level EXEC	All
show authentication	Displays the authentication configuration.	User-level EXEC & privileged-level EXEC	All
show authsvr	Displays the Authorization Server status.	User-level EXEC & privileged-level EXEC	SE
show bandwidth	Displays the bandwidth allocated to a particular device.	User-level EXEC & privileged-level EXEC	SE, SR
show banner	Displays information on various types of banners.	User-level EXEC & privileged-level EXEC	All
show bitrate	Displays the SE bit-rate configuration.	User-level EXEC & privileged-level EXEC	SE, SR
show cache	Displays a list of cached contents.	User-level EXEC & privileged-level EXEC	SE
show capability	Displays information for the Cap-X profile ID.	User-level EXEC & privileged-level EXEC	SE
show cdnfs	Displays the Internet Streamer CDS network file system information.	User-level EXEC & privileged-level EXEC	SE, CDSM
show clock	Displays the system clock.	User-level EXEC & privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
show cms	Displays the Centralized Management System protocol, embedded database content, maintenance status, and other information.	User-level EXEC & privileged-level EXEC	All
show content	Displays all content entries in the CDS.	User-level EXEC & privileged-level EXEC	SE
show debugging	Displays the state of each debugging option the state of each debugging option.	User-level EXEC & privileged-level EXEC	All
show device-mode	Displays the configured or current mode of a CDSM, SE, or SR device.	User-level EXEC & privileged-level EXEC	All
show direct-server-return	Displays the Direct Server return information.	User-level EXEC & privileged-level EXEC	SE, SR
show disks	Displays the disk configurations.	User-level EXEC & privileged-level EXEC	All
show distribution	Displays the distribution information for a specified delivery service.	User-level EXEC & privileged-level EXEC	SE
show flash	Displays the flash memory information.	User-level EXEC & privileged-level EXEC	All
show flash-media-streaming	Displays the Flash Media Streaming information.	User-level EXEC & privileged-level EXEC	SE, SR
show ftp	Displays the caching configuration of the File Transfer Protocol (FTP).	User-level EXEC & privileged-level EXEC	All
show hardware	Displays the system hardware information.	Privileged-level EXEC	All
show hosts	Displays the IP domain name, name servers, IP addresses, and host table.	User-level EXEC & privileged-level EXEC	All
show http	Displays the HTTP-related caching configuration.	User-level EXEC & privileged-level EXEC	SE
show icap	Displays the ICAP configurations.	User-level EXEC & privileged-level EXEC	SE

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
show interface	Displays the hardware interface information.	User-level EXEC & privileged-level EXEC	All
show inventory	Displays the system inventory information.	User-level EXEC & privileged-level EXEC	All
show ip access-list	Displays the information about access lists that are defined and applied to specific interfaces or applications.	Privileged-level EXEC	SE
show ip routes	Displays the IP routing table.	Privileged-level EXEC	All
show ldap	Displays the LDAP parameters.	User-level EXEC & privileged-level EXEC	SE
show logging	Displays the system logging configuration.	User-level EXEC & privileged-level EXEC	All
show movie-streamer	Displays the Movie Streamer configuration.	User-level EXEC & privileged-level EXEC	SE
show ntp	Displays the Network Time Protocol configuration status.	User-level EXEC & privileged-level EXEC	All
show processes	Displays the process status.	User-level EXEC & privileged-level EXEC	All
show programs	Displays the scheduled programs.	User-level EXEC & privileged-level EXEC	SE
show qos	Displays QoS information.	User-level EXEC & privileged-level EXEC	SE
show radius-server	Displays the RADIUS server information.	User-level EXEC & privileged-level EXEC	All
show rea	Displays the REA information.	User-level EXEC & privileged-level EXEC	SE
show rcp	Displays RCP information	User-level EXEC & privileged-level EXEC	All
show rtsp	Displays the RTSP configurations.	User-level EXEC & privileged-level EXEC	SE

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
show rule	Displays the Rules Template configuration information.	User-level EXEC & privileged-level EXEC	SE
show running-config	Displays the current operating configuration.	User-level EXEC & privileged-level EXEC	All
show service-router	Displays the service router configuration.	User-level EXEC & privileged-level EXEC	All
show services	Displays the services-related information.	User-level EXEC & privileged-level EXEC	All
show snmp	Displays the SNMP parameters.	User-level EXEC & privileged-level EXEC	All
show ssh	Displays the Secure Shell status and configuration.	User-level EXEC & privileged-level EXEC	All
show standby	Displays the information related to the standby interface.	User-level EXEC & privileged-level EXEC	All
show startup-config	Displays the startup configuration.	User-level EXEC & privileged-level EXEC	All
show statistics access-lists 300	Displays the access control list statistics.	User-level EXEC & privileged-level EXEC	SE
show statistics acquirer	Displays the SE acquirer delivery service statistics.	User-level EXEC & privileged-level EXEC	SE
show statistics authentication	Displays the authentication statistics.	User-level EXEC & privileged-level EXEC	SE
show statistics cdnfs	Displays the SE Internet Streamer CDS network file system statistics.	User-level EXEC & privileged-level EXEC	SE, CDSM
show statistics distribution	Displays the simplified statistics for content distribution components.	User-level EXEC & privileged-level EXEC	SE
show statistics flash-media-streaming	Displays the statistics for Flash Media Streaming.	User-level EXEC & privileged-level EXEC	SE

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
show statistics http	Displays the Hypertext Transfer Protocol statistics.	User-level EXEC & privileged-level EXEC	SE, SR
show statistics icap	Displays the ICAP-related statistics.	User-level EXEC & privileged-level EXEC	SE
show statistics icmp	Displays the Internet Control Message Protocol statistics.	User-level EXEC & privileged-level EXEC	All
show statistics ip	Displays the Internet Protocol statistics.	User-level EXEC & privileged-level EXEC	All
show statistics movie-streamer	Displays statistics for the Movie Streamer.	User-level EXEC & privileged-level EXEC	SE
show statistics netstat	Displays the Internet socket connection statistics.	User-level EXEC & privileged-level EXEC	All
show statistics qos	Displays statistics for the QoS policy service.	User-level EXEC & privileged-level EXEC	SE
show statistics radius	Displays the RADIUS authentication statistics.	User-level EXEC & privileged-level EXEC	All
show statistics replication	Displays the delivery service replication status and related statistical data.	User-level EXEC & privileged-level EXEC	SE, CDSM
show statistics service-router	Displays the Service Router statistics.	User-level EXEC & privileged-level EXEC	SR
show statistics services	Displays the services statistics.	User-level EXEC & privileged-level EXEC	All
show statistics snmp	Displays the SNMP statistics.	User-level EXEC & privileged-level EXEC	All
show statistics tacacs	Displays the Service Engine TACACS+ authentication and authorization statistics.	User-level EXEC & privileged-level EXEC	All
show statistics tcp	Displays the Transmission Control Protocol statistics.	User-level EXEC & privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
show statistics transaction-logs	Displays the transaction log export statistics.	User-level EXEC & privileged-level EXEC	SE
show statistics udp	Displays the User Datagram Protocol statistics.	User-level EXEC & privileged-level EXEC	All
show statistics wmt	Displays the Windows Media Technologies statistics.	User-level EXEC & privileged-level EXEC	SE
show tacacs	Displays TACACS+ authentication protocol configuration information.	User-level EXEC & privileged-level EXEC	All
show tech-support	Displays the system information for Cisco technical support.	User-level EXEC & privileged-level EXEC	All
show telnet	Displays the Telnet services configuration.	User-level EXEC & privileged-level EXEC	All
show transaction-logging	Displays the transaction logging information.	User-level EXEC & privileged-level EXEC	SE
show url-signature	Displays the URL signature information.	User-level EXEC & privileged-level EXEC	SE
show user	Displays the user identification number and username information.	User-level EXEC & privileged-level EXEC	All
show users	Displays the specified users.	User-level EXEC & privileged-level EXEC	All
show version	Displays the software version.	User-level EXEC & privileged-level EXEC	All
show wmt	Displays the WMT configuration.	User-level EXEC & privileged-level EXEC	SE
shutdown (interface configuration)	Shuts down the specified interface.	interface configuration	All
shutdown (EXEC)	Shuts down the device (stops all applications and operating system).	Privileged-level EXEC	All
snmp-server community	Configures the community access string to permit access to the SNMP.	Global configuration	All
snmp-server contact	Specifies the text for the MIB object sysContact.	Global configuration	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
snmp-server enable traps	Enables the SNMP traps.	Global configuration	All
snmp-server group	Defines a user security model group.	Global configuration	All
snmp-server host	Specifies the hosts to receive SNMP traps.	Global configuration	All
snmp-server location	Specifies the path for the MIB object sysLocation.	Global configuration	All
snmp-server notify inform	Configures the SNMP inform request.	Global configuration	All
snmp-server user	Defines a user who can access the SNMP engine.	Global configuration	All
snmp-server view	Defines a Version 2 SNMP (SNMPv2) MIB view.	Global configuration	All
sshd	Configures the SSH service parameters.	Global configuration	All
sysreport	Saves the sysreport onto a user-specified file.	Privileged-level EXEC	SE
tacacs	Configures TACACS+ server parameters.	Global configuration	All
tcpdump	Dumps the TCP traffic on the network.	Privileged-level EXEC	All
telnet	Starts the Telnet client.	User-level EXEC & privileged-level EXEC	All
telnet enable	Enables the Telnet services.	Global configuration	All
terminal	Sets the terminal output commands.	User-level EXEC & privileged-level EXEC	All
test-url	Tests the accessibility of a URL using FTP, HTTP, or HTTPS.	User-level EXEC & privileged-level EXEC	SE, SR
traceroute	Traces the route to a remote host.	User-level EXEC & privileged-level EXEC	All
traceroute6	Traces the route to a remote IPv6-enabled host.	User-level EXEC & privileged-level EXEC	SE, SR
transaction-log force	Forces archiving of the working log file to make a transaction log file.	Privileged-level EXEC	All
transaction-logs	Configures and enables the transaction logging parameters.	Global configuration	SE

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
type	Displays a file.	User-level EXEC & privileged-level EXEC	All
type-tail	Displays the last several lines of a file.	User-level EXEC & privileged-level EXEC	All
undebug	Disables the debugging functions (see also **debug**).	Privileged-level EXEC	All
url-signature	Configures the url signature,	Global configuration	SE
username	Establishes the username authentication.	Global configuration	All
whoami	Displays the current user's name.	User-level EXEC & privileged-level EXEC	All
wmt	Configures the WMT.	Global configuration	SE
write	Writes or erases the startup configurations to NVRAM or to a terminal session, or writes the MIB persistence configuration to disk.	Privileged-level EXEC	All

1. Commands used to access configuration modes.

access-lists

To configure access control list entries, use the **access-lists** global configuration command. To remove access control list entries, use the **no** form of this command.

access-lists {**300** {**deny groupname** {**any** [**position** *number*] | *groupname* [**position** *number*]}} | {**permit groupname** {**any** [**position** *number*] | *groupname* [**position** *number*]}} | **enable**}

no access-lists {**300** {**deny groupname** {**any** [**position** *number*] | *groupname* [**position** *number*]}} | {**permit groupname** {**any** [**position** *number*] | *groupname* [**position** *number*]}} | **enable**}

Syntax Description

300	Specifies the group name-based access control list (ACL).
deny	Specifies the rejection action.
groupname	Defines which groups are granted or denied access to content that is served by this SE.
any	Specifies any group name.
position	(Optional) Specifies the position of the access control list record within the access list.
number	Position number within the access control list (1–4294967294).
groupname	Name of the group that is permitted or denied from accessing the Internet using an SE.
permit	Specifies the permission action.
enable	Enables the access control list.

Defaults

No default behavior or values.

Command Modes

Global configuration

Usage Guidelines

In the Internet Streamer CDS 2.x software, you can configure group authorization using an access control list (ACL) only after a user has been authenticated against an LDAP HTTP-request authentication server. The use of this list configures a group privilege when members of the group are accessing content provided by the SE. You can use the ACL to allow the users who belong to certain groups or to prevent them from viewing specific content. This authorization feature offers more granular access control by specifying that access is only allowed to specific groups.

Use the **access-lists enable** global configuration command to enable the use of the ACL.

Use the **access-lists 300** command to permit or deny a group from accessing the Internet using the SE. For instance, use the **access-lists 300 deny groupname marketing** command to prevent any user from the marketing group from accessing content through the SE.

At least one login authentication method, such as local, TACACS+, or RADIUS, must be enabled.

Note We recommend that you configure the local login authentication method as the primary method.

In Cisco Internet Streamer Release 2.4 software, the access control list contains the following feature enhancements and limitations:

- A user can belong to several groups.
- A user can belong to an unlimited number of groups within group name strings.
- A group name string is a case-sensitive string with mixed-case alphanumeric characteristics.
- Each unique group name string cannot exceed 128 characters.

Note If the unique group name string is longer than 128 characters, the group is ignored.

- The group names in a group name string are separated by a comma.
- The total string of individual group names cannot exceed 750 characters.

For Windows-based user groups, you must append the domain name in front of the group name in the form domain or group as follows:

For Windows NT-based user groups, use the domain NetBIOS name.

Examples

The following example shows how to display the configuration of the access control list by using the **show access-lists 300** command:

```
ServiceEngine#show access-lists 300
Access Control List Configuration
  ---------------------------------
    Access Control List is enabled

    Groupname-based List (300)
    1. permit groupname techpubs
    2. permit groupname acme1
    3. permit groupname engineering
    4. permit groupname sales
    5. permit groupname marketing
    6. deny groupname any
```

The following example shows how to display statistical information for the access control list by using the **show statistics access-lists 300** command:

```
ServiceEngine#show statistics access-lists 300
    Access Control Lists Statistics
    -----------------------------------------
      Groupname and username-based List (300)
        Number of requests:         1
        Number of deny responses:   0
        Number of permit responses: 1
```

The following example shows how to reset the statistical information for the access control list by using the **clear statistics access-lists 300** command:

```
ServiceEngine#clear statistics access-lists 300
ServiceEngine(config)#access-lists 300 permit groupname acme1 position 2
```

Related Commands

show access-lists 300
show statistics access-list 300

acquirer (EXEC)

To start or stop content acquisition on a specified acquirer delivery service, use the **acquirer** EXEC command. You can also use this command to verify and correct the Last-Modified-Time attribute in content acquired using the Cisco Internet Streamer CDS software.

acquirer {**check-time-for-old-content** [**delivery-service-id** *delivery-service-num* | **delivery-service-name** *delivery-service-name*] | [**correct** [**delivery-service-id** *delivery-service-num* | **delivery-service-name** *delivery-service-name*]] | **start-delivery-service** {**delivery-service-id** *delivery-service-num* | **delivery-service-name** *delivery-service-name*} | **stop-delivery-service** {**delivery-service-id** *delivery-service-num* | **delivery-service-name** *delivery-service-name*} | **test-url** *url* [**use-http-proxy** *url* | **use-smb-options** *smb-options*]}

Syntax Description

check-time-for-old-content	Checks the content for Last-Modified-Time attributes in the local time format.
delivery-service-id	(Optional) Sets the delivery service number identifier.
delivery-service-num	(Optional) Delivery service number (0–4294967295).
delivery-service-name	(Optional) Sets the delivery service name descriptor.
delivery-service-name	(Optional) Delivery service name.
correct	(Optional) Changes the Last-Modified-Time attributes in the local time format to the Greenwich mean time (GMT) format.
start-delivery-service	Starts the content acquisition.
stop-delivery-service	Stops the content acquisition.
test-url	Tests the accessibility of a URL, using HTTP, HTTPS, FTP, or SMB.
url	URL to be tested. **Note** For the Server Message Block (SMB) protocol, use the uniform naming convention (UNC) path, for example, //host/share/file.
use-http-proxy	(Optional) Specifies the HTTP proxy. The connectivity of the URL (content request over HTTP) through the HTTP proxy server (the SE) is tested. Use this option only when the HTTP protocol is used.
url	HTTP proxy URL. Use one of the following formats to specify the HTTP proxy URL: http://*proxyIpAddress*:*proxyPort* http://*proxyUser*:*proxypasswd*@*proxyIpAddress*:*proxyPort*
use-smb-options	(Optional) Specifies the username, password, port, and domain for the SMB URL.
smb-options	Parameters to be specified when an SMB URL is used. Use the following format to specify these parameters: username=xxx,password=xxx,port=xxx,workgroup=xxx **Note** All the comma-separated key=value pairs are optional and need to be specified only if the SMB host requires them.

Defaults

If you do not specify the delivery service, this command applies to all delivery services assigned to the root SE.

Command Modes

EXEC

Usage Guidelines

The acquirer is a software agent that gathers delivery service content before it is distributed to the receiver SEs in an Internet Streamer CDS network. The acquirer maintains a task list, which it updates after receiving a notification of changes in its delivery service configuration.

The acquirer stores the Last-Modified-Time attribute in the local time format. Content acquired using earlier software releases has a Last-Modified-Time attribute that is incorrect if used with later versions of the Internet Streamer CDS software, which use GMT format.

With Internet Streamer CDS Release 2.4 software, you must correct the Last-Modified-Time attributes for content acquired with earlier releases by entering the following command from the privileged EXEC prompt:

acquirer check-time-for-old-content correct [**delivery-service-id** *delivery-service-num* **delivery-service-name** *delivery-service-name*]

This command changes the Last-Modified-Time attributes for content in all delivery services assigned to the root SE unless you specify the delivery service ID or name.

SEs running Internet Streamer CDS Release 2.4 software identify changes in the Last-Modified-Time attribute and download content only when changes have occurred.

Use the **acquirer start-delivery-service** command to immediately start acquisition tasks for the selected delivery-service. Use the **acquirer stop-delivery-service** command to immediately stop all acquisition tasks for the selected delivery service.

Use the **acquirer test-url** *url* EXEC command to test whether a URL is accessible or not. The actual content is dumped into the path /dev/null.

Examples

The following example shows how the acquirer starts acquiring content on delivery service 86:

```
ServiceEngine#acquirer start-delivery-service delivery-service-id 86

ServiceEngine#acquirer start-delivery-service delivery-service-name corporate
```

The following example shows how the acquirer stops acquiring content on delivery service 86:

```
ServiceEngine#acquirer stop-delivery-service delivery-service-id 86

ServiceEngine#acquirer stop-delivery-service delivery-service-name corporate
```

The following example shows how the **acquirer test-url** command is used to test a URL:

```
ServiceEngine#acquirer test-url http://172.16.150.26
--05:16:41--  http://10.107.150.26
           => `/dev/null'
Connecting to 10.107.150.26:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1,722 [text/html]

100%[====================================>] 1,722          1.64M/s    ETA 00:00

02:45:40 (1.64 MB/s) - `/dev/null' saved [1722/1722]
```

Related Commands

show acquirer
show statistics acquirer

acquirer (global configuration)

To provide authentication when the acquirer obtains content through a proxy server, use the **acquirer** global configuration command. To disable acquirer proxy authentication, use the **no** form of this command.

acquirer proxy authentication {**outgoing** {*hostname* | *ip-address*} *port-num*} *username* | **password** *password*}

no acquirer proxy authentication {**outgoing** {*hostname* | *ip-address*} *port-num*} *username* | **password** *password*}

Syntax Description

proxy	Configures parameters for outgoing proxy-mode requests for content acquisition.
authentication	Enables authentication so the acquirer can obtain content through a proxy server.
outgoing	Enables authentication for a nontransparent proxy server.
hostname	Hostname of a nontransparent proxy server.
ip-address	IP address of a nontransparent proxy server.
port-num	Port number of a nontransparent proxy server (1–65535).
username	Username for authentication using a maximum of 256 characters.
password	Allows the use of a password for authentication.
password	Password for authentication using a maximum of 256 characters.

Defaults

No default behavior or values.

Command Modes

Global configuration

Usage Guidelines

Use the **acquirer proxy authentication outgoing** global configuration command to configure authentication when you enable content acquisition through a proxy server. You must first configure the proxy host and the port using the **http proxy outgoing host** global configuration command. The maximum number of outgoing proxies allowed is eight. When you remove an outgoing proxy using the **no http outgoing proxy** command, the authentication information associated with that proxy is automatically removed.

Use the **acquirer proxy authentication transparent** command for transparent caches in the Internet Streamer CDS network that require authentication.

The acquirer supports a proxy with basic authentication. Content acquisition through a proxy server is supported only for HTTP and not for HTTPS or FTP. Also, authentication is only supported for a single proxy server in a chain, so if multiple proxy servers in a chain require authentication, the request will fail.

Acquisition through a proxy server can be configured when the root SE cannot directly access the origin server because the origin server is set up to allow access only by a specified proxy server. When a proxy server is configured for root SE content acquisition, the acquirer contacts the proxy server instead of the origin server, and all requests to that origin server go through the proxy server.

Note Content acquisition through a proxy server is only supported for HTTP requests. It is not supported for HTTPS, FTP, MMS, or MMS-over-HTTP requests.

There are three ways to configure the proxy server: through the CDSM GUI, through the SE CLI, or through the manifest file. If you need to configure the SE to use the proxy for both caching and pre-positioned content, use the CLI to configure the proxy. The CLI command is a global configuration command that configures the entire SE to use the proxy. If only the acquirer portion of the SE needs to use the proxy for acquiring the pre-positioned content, use the manifest file or specify the outgoing proxy. When you configure the proxy server in the manifest file, you are configuring the acquirer to use the proxy to fetch the content for a particular delivery service.

Note Proxy configurations in the manifest file take precedence over proxy configurations in the CLI. A *noProxy* attribute configuration in the manifest file takes precedence over the other proxy server configurations in the manifest file.

You can also configure a proxy for fetching the manifest file by using the CDSM GUI (the Creating New Delivery Service or Modifying Delivery Service window). When you configure a proxy server in the CDSM GUI, the proxy configuration is valid only for acquiring the manifest file itself and not for acquiring the delivery service content. Requests for the manifest file go through the proxy server, and requests for the content go directly to the origin server.

Tip Before configuring a proxy server, verify that the root SE is able to ping the proxy server. To check whether the proxy server is accepting incoming HTTP traffic at the configured port, use the **acquirer test-url http://***proxyIP***:***proxyport* global configuration command in the root SE CLI, where the URL in the command is the URL of the proxy server being tested. If the proxy is not servicing the configured port, this message displays “failed: Connection refused.”

Examples

The following example shows the authentication configuration for a transparent proxy server with basic authentication:

```
ServiceEngine(config)#acquirer proxy authentication transparent 192.168.1.1 8080 myname
```

Related Commands

http proxy outgoing
show acquirer

acquisition-distribution

To start or stop the content acquisition and distribution process, use the **acquisition-distribution** EXEC command.

acquisition-distribution {**database-cleanup** {**start** | **stop**} | **start** | **stop**}

Syntax Description

database-cleanup	Cleans up the acquisition and distribution database to maintain consistency with the file system.
start	Starts the cleanup of the acquisition and distribution database.
stop	Stops the cleanup of the acquisition and distribution database.
start	Starts the acquisition and distribution process.
stop	Stops the acquisition and distribution process.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

When you use the **acquisition-distribution database-cleanup** command, the acquisition and distribution database is checked to ensure that all pre-positioned content is available in cdnfs. If any pre-positioned content is found to be missing from cdnfs, the content is replicated to all SEs in the Internet Streamer CDS network. Root SEs assigned to a delivery service acquire the content directly from the origin server and replicate the content through the delivery service either by unicast or multicast transmission to other SEs in the delivery service. Receiver SEs obtain the content from forwarder SEs either by unicast or multicast. In the case of a disk00 failure when the database is stored on disk00 in an internal file system (/state), the recovery of the acquisition and distribution database is done automatically. You should run the acquisition and distribution database cleanup if a failure occurs or if you have to replace a disk drive other than disk00.

Examples

The following example starts the acquisition and distribution database cleanup process:

```
ServiceEngine#acquisition-distribution database-cleanup start
```

The following example starts the acquisition and distribution process:

```
ServiceEngine#acquisition-distribution start
```

The following example stops the acquisition and distribution process:

```
ServiceEngine#acquisition-distribution stop
```

Related Commands

cdnfs cleanup
show acquirer
show distribution

alarm overload-detect

To detect alarm overload situations, use the **alarm overload-detect** global configuration command. To disable alarm overload detection, use the **no** form of this command.

alarm overload-detect {**clear** *1-999* [**raise** *10-1000*] | **enable** | **raise** *10-1000* [**clear** *1-999*]}

no alarm overload-detect {**clear** *1-999* [**raise** *10-1000*] | **enable** | **raise** *10-1000* [**clear** *1-999*]}

Syntax Description

clear	Specifies the threshold below which the alarm overload state on the SE is cleared and the SNMP traps and alarm notifications to the Centralized Management System (CMS) resume. **Note** The **alarm overload-detect clear** value must be less than the **alarm overload-detect raise** value.
1-999	Number of alarms per second that ends an alarm overload condition.
raise	(Optional) Specifies the threshold at which the CDE enters an alarm overload state and SNMP traps and alarm notifications to CMS are suspended.
10-1000	Number of alarms per second that triggers an alarm overload.
enable	(Optional) Enables the detection of alarm overload situations.

Defaults

raise: 10 alarms per second

clear: 1 alarm per second

Command Modes

Global configuration

Usage Guidelines

When multiple applications running on an SE experience problems at the same time, numerous alarms are set off simultaneously, and the SE may stop responding. In the Internet Streamer CDS 2.2 software and later releases, you can use the **alarm overload-detect** global configuration command to set an overload limit for the incoming alarms from the node health manager. If the number of alarms exceeds the maximum number of alarms allowed, the SE enters an alarm overload state until the number of alarms drops down to the number defined in the **clear** option.

When the SE is in the alarm overload state, the following events occur:

- An alarm overload notification is sent to SNMP and the CMS. The **clear** and **raise** values are also communicated to SNMP and the CMS.
- SNMP traps and CMS notifications for subsequent alarm raise and clear operations are suspended.
- An alarm overload clear notification is sent.
- The SE remains in the alarm overload state until the rate of incoming alarms decreases to the **clear** value.

Note In the alarm overload state, applications continue to raise alarms and the alarms are recorded within the SE. The **show alarms** and **show alarms history** EXEC commands will display all the alarms even in the alarm overload state.

Examples

The following example enables the detection of alarm overload:

```
ServiceEngine(config)#alarm overload-detect enable
```

The following example sets the threshold for triggering the alarm overload at 100 alarms per second:

```
ServiceEngine(config)#alarm overload-detect raise 100
```

The following example sets the level for clearing the alarm overload at 10 alarms per second:

```
ServiceEngine(config)#alarm overload-detect clear 10
```

Related Commands

show alarms
show alarm status

asset

To to configure the CISCO-ENTITY-ASSET-MIB, use the **asset** global configuration command. To remove the asset tag name, use the **no** form of this command.

asset tag *name*

no asset tag *name*

Syntax Description

tag	Sets the asset tag.
name	Asset tag name string.

Defaults

No default behavior or values.

Command Modes

Global configuration

Examples

The following example shows how to configure a tag name for the asset tag string:

```
ServiceEngine(config)#asset tag entitymib
```

authentication

To specify authentication and authorization methods, use the **authentication** command in global configuration mode. To selectively disable options, use the **no** form of this command.

authentication {**configuration {local** | **radius** | **tacacs**} **enable** [**primary** | **secondary**] | **fail-over server-unreachable** | **login** {**local** | **radius** | **tacacs**} **enable** [**primary** | **secondary**] }

no authentication {configuration {local | **radius** | **tacacs**} **enable** [**primary** | **secondary**] | **fail-over server-unreachable** | **login** {**local** | **radius** | **tacacs**} **enable** [**primary** | **secondary**] }

Syntax Description

configuration	Sets configuration authentication (authorization).
local	Selects the local database for authentication or authorization.
radius	Selects a RADIUS server for authentication or authorization.
tacacs	Selects TACACS+ server authentication.
enable	Enables the source of authorization information.
primary	(Optional) Sets the first authentication method used.
secondary	(Optional) Sets the second authentication method used.
fail-over	Sets the condition to use the next authentication scheme, when primary authentication fails.
server-unreachable	Specifies that a failover to the secondary authentication scheme should occur only if the primary authentication server is unreachable.
login	Selects the local method for authentication.

Command Defaults

The local authentication method is enabled by default.

Command Modes

Global configuration

Usage Guidelines

Authentication, also referred to as login, is the act of verifying usernames and passwords. Authorization is the action of determining what a user is allowed to do. It permits or denies privileges for authenticated users in the network. For example, if you log in to an SE with a superuser administrator account (for example, the predefined admin account), you have the highest level of access privileges and can perform any administrative task such as the following:

- Configure the standalone SE.
- Obtain statistical information that the standalone SE has collected.
- Reload the device.

Generally, authentication precedes authorization in a network.

The **authentication** command configures both the authentication and authorization methods that govern login and configuration access to the SE. Login and configuration privileges can be maintained in two different databases in the Internet Streamer CDS 2.5 software: the local database, TACACS+ database, and RADIUS database. If all databases are enabled, then all three databases are queried. If the user data cannot be found in the first database queried, then the second and third databases are queried.

When an administrator can log in to the SE through the console or the GUI, the SE checks the specified authentication database to verify the user's username and password to process these administrative login requests and to determine the access rights that this particular administrator should be granted during this login session. When the SE receives an administrative login request, the SE can check its local database or a remote third-party database (the TACACS+ database or the RADIUS database) to verify the username with the password and to determine the access privileges of the administrator.

When defining or modifying the authentication configuration method for an SE, follow these guidelines:

- You can use the **authentication** command to choose between using an external access server or the internal (local) SE-based AAA system for user access management.
- You can configure any combination of these authentication and authorization methods to control access and set privileges on an SE:
  - Local authentication and authorization
  - RADIUS authentication and authorization
  - TACACS+ authentication and authorization
- Authentication configuration applies to the following:
  - Console and Telnet connection attempts
  - Secure FTP (SFTP), SSH (SSH Version 1 and Version 2), and Websense server access
- If you configure a RADIUS or TACACS+ key on the SE (the RADIUS client), make sure that you configure an identical key on the RADIUS or TACACS+ server.
- If you configure multiple RADIUS or TACACS+ servers, the first server configured is the primary server, and authentication requests are sent to this server first. You can also specify secondary servers for authentication and authorization purposes.
- By default, the SE uses the local database to authenticate and authorize administrative login requests. The SE verifies whether all authentication databases are disabled and if so, sets the system to the default state. For information on this default state, see the "Default Administrative Login Authentication and Authorization Configuration" section on page 2-27.

The **authentication login** command determines whether the user has any level of permission to access the SE. The **authentication configuration** command authorizes the user with privileged access (configuration access) to the SE.

The **authentication login local** and the **authentication configuration local** commands use a local database for authentication and authorization.

The **authentication login tacacs** and **authentication configuration tacacs** commands use a remote TACACS+ server to determine the level of user access.

The TACACS+ database validates users before they gain access to an SE. TACACS+ is derived from the United States Department of Defense (RFC 1492) and is used by Cisco as an additional control of nonprivileged and privileged mode access. The Cisco Internet Streamer CDS 2.4 and later software releases support TACACS+ only and not TACACS or Extended TACACS.

To configure TACACS+, use the **authentication** and **tacacs** commands. To enable TACACS+, use the **tacacs enable** command.

For more information on TACACS+ authentication, see the "tacacs" section on page 403.

The authentication login radius and authentication configuration radius commands use a remote RADIUS server to determine the level of user access.

The **authentication login tacacs** and **authentication configuration tacacs** commands use a remote TACACS+ server to determine the level of user access.

By default, the local method is enabled, with TACACS+ and RADIUS both disabled for login and configuration. Whenever TACACS+ and RADIUS are disabled, local is automatically enabled. TACACS+, RADIUS and local methods can be enabled at the same time. The **primary** option specifies the first method to attempt for both login and configuration; the **secondary** option specifies the method to use if the primary method fails. If all methods of an **authentication login** or **authentication configuration** commands are configured as primary or secondary, local is attempted first, then TACACS+ and then RADIUS.

Note You must use the **tacacs** global configuration command to configure a TACACS+ server for the TACACS+ authentication and authorization method. For information about configuring a TACACS+ server, see the "Specifying TACACS+ Authentication and Authorization Settings" section on page 2-44.

You must use the **radius-server** global configuration command to configure a RADIUS server for the RADIUS authentication and authorization method. For information about configuring a RADIUS server, see the "Specifying RADIUS Authentication and Authorization Settings" section on page 2-28.

Default Administrative Login Authentication and Authorization Configuration

By default, the SE uses the local database to obtain login authentication and authorization privileges for administrative users.

Note Use the **authentication** command to configure the authentication methods that govern administrative login and configuration access to the SE.

Table 2-2 lists the default configuration for administrative login authentication and authorization.

Table 2-2 Default Configuration for Administrative Login Authentication and Authorization

Feature	Default Value
Administrative login authentication	Enabled
Administrative configuration authorization	Enabled
Authentication server failover because the authentication server is unreachable	Disabled
TACACS+ login authentication (console and Telnet)	Disabled
TACACS+ authorization (console and Telnet)	Disabled
TACACS+ key	None specified
TACACS+ server timeout	5 seconds
TACACS+ retransmit attempts	2 times
RADIUS login authentication (console and Telnet)	Disabled
RADIUS authorization (console and Telnet)	Disabled
RADIUS server IP address	None specified
RADIUS server UDP authorization port	Port 1645
RADIUS key	None specified

Table 2-2 Default Configuration for Administrative Login Authentication and Authorization (continued)

Feature	Default Value
RADIUS server timeout	5 seconds
RADIUS retransmit attempts	2 times

Enforcing Authentication with the Primary Method

The **authentication fail-over server-unreachable** command allows you to specify that failover to the secondary authentication method should occur only if the primary authentication server is unreachable. This feature ensures that users gain access to the SE using the local database only when nonlocal authentication servers are (TACACS+ or RADIUS) are unreachable. For example, when a TACACS+ server is enabled for authentication with user authentication failover configured and the user tries to log in to the SE using an account defined in the local database, login fails. Login succeeds only when the TACACS+ server is unreachable.

Server Redundancy

You can specify authentication servers with the corresponding authentication server (LDAP, or RADIUS) **host** command options, or in the case of TACACS+ servers, with the server hostname command option, to configure additional servers. These additional servers provide authentication redundancy and improved throughput, especially when SE load-balancing schemes distribute the requests evenly between the servers. If the SE cannot connect to any of the authentication servers, no authentication takes place and users who have not been previously authenticated are denied access.

Login Authentication and Authorization Through the Local Database

Local authentication and authorization use locally configured login and passwords to authenticate administrative login attempts. The login and passwords are local to each SE and are not mapped to individual usernames.

By default, local login authentication is enabled first. You can disable local login authentication only after enabling one or more of the other administrative login authentication methods. However, when local login authentication is disabled, if you disable all other administrative login authentication methods, local login authentication is reenabled automatically.

Specifying RADIUS Authentication and Authorization Settings

RADIUS authentication clients reside on the SE running Cisco Internet Streamer Release 2.5 software. When enabled, these clients send authentication requests to a central (remote) RADIUS server, which contains login authentication and network service access information.

To configure RADIUS authentication on an SE, you must configure a set of RADIUS authentication server settings on the SE. You can use the GUI or the CLI to configure this set of RADIUS authentication server settings for an SE.

Table 2-3 describes the RADIUS authentication settings.

Table 2-3 RADIUS Authentication Settings

Setting	Description
RADIUS server	RADIUS servers that the SE is to use for RADIUS authentication. To enable the SE to use a specific RADIUS server, enter the IP address or hostname of the RADIUS server and port information. Up to five different hosts are allowed. Early deployment of RADIUS was done using port number 1645, although the official port number for RADIUS is now 1812. Up to five different ports are allowed.
RADIUS key	Key used to encrypt and authenticate all communication between the RADIUS client (the SE) and the RADIUS server. The maximum number of characters in the key is 15. There is no default. **Tip** Make sure that the same RADIUS key is enabled on the RADIUS server.
RADIUS timeout interval	Number of seconds that the SE waits for a response from the specified RADIUS authentication server before declaring a timeout. The range is 1 to 20 seconds. The default value is 5 seconds.
RADIUS retransmit count	Number of times that the SE is to retransmit its connection to the RADIUS if the RADIUS timeout interval is exceeded. The range is one to three tries. The default value is two tries.

After configuring these RADIUS authentication settings on the SE, you can enable RADIUS login authentication and authorization on the SE.

Specifying TACACS+ Authentication and Authorization Settings

TACACS+ controls access to network devices by exchanging Network Access Server (NAS) information between a network device and a centralized database to determine the identity of a user or an entity. TACACS+ is an enhanced version of TACACS, a UDP-based access-control protocol specified by RFC 1492. TACACS+ uses TCP to ensure reliable delivery and encrypt all traffic between the TACACS+ server and the TACACS+ daemon on a network device.

TACACS+ works with many authentication types, including fixed password, one-time password, and challenge-response authentication.

When a user requests restricted services, TACACS+ encrypts the user password information using the MD5 encryption algorithm and adds a TACACS+ packet header. This header information identifies the packet type being sent (for example, an authentication packet), the packet sequence number, the encryption type used, and the total packet length. The TACACS+ protocol then forwards the packet to the TACACS+ server.

A TACACS+ server can provide authentication, authorization, and accounting functions. These services, while all part of TACACS+, are independent of one another. A TACACS+ configuration can use any or all of the three services.

When the TACACS+ server receives a packet, it does the following:

- Authenticates the user information and notifies the client that the login authentication has either succeeded or failed.
- Notifies the client that authentication will continue and that the client must provide additional information. This challenge-response process can continue through multiple iterations until login authentication either succeeds or fails.

You can configure a TACACS+ key on the client and server. If you configure a key on the SE, it must be the same as the one configured on the TACACS+ servers. The TACACS+ clients and servers use the key to encrypt all TACACS+ packets transmitted. If you do not configure a TACACS+ key, packets are not encrypted.

TACACS+ authentication is disabled by default. You can enable TACACS+ authentication and local authentication at the same time.

In order to configure TACACS+ authentication on SEs, you must configure a set of TACACS+ authentication settings on the SE. You can use the SE CLI or GUI to configure this set of TACACS+ authentication settings for a SE.

Table 2-4 describes the TACACS+ authentication settings.

Note No TACACS+ authentication will be performed if no TACACS+ servers are configured on the SE.

Table 2-4 TACACS+ Authentication Settings

Setting	Description
TACACS+ server	TACACS+ servers that the SE uses for TACACS+ authentication. Explicitly specify the primary TACACS+ server; otherwise, the SE makes its own decision. You can configure one primary TACACS+ server and two backup TACACS+ servers. TACACS+ uses the standard port (port 49) for communication, based on the specified service.
TACACS+ key	Secret key that the SE uses to communicate with the TACACS+ server. The maximum number of characters in the TACACS+ key should not exceed 99 printable ASCII characters (except tabs). An empty key string is the default. All leading spaces are ignored; spaces within and at the end of the key string are not ignored. Double quotes are not required even if there are spaces in the key, unless the quotes themselves are part of the key. There is no default. **Tip** Make sure that the same TACACS+ key is specified on the TACACS+ server.
TACACS+ timeout interval	Number of seconds that the SE waits for a response from the specified TACACS+ authentication server before declaring a timeout. The range is 1 to 20 seconds. The default value is 5 seconds.
TACACS+ retransmit count	Number of times that the SE retransmits its connection to the TACACS+ if the TACACS+ timeout interval is exceeded. The range is one to three tries. The default value is two tries.
TACACS+ password authentication method	Mechanism for password authentication. By default, the Password Authentication Protocol (PAP) is the mechanism for password authentication. The other option is to use ASCII clear text as the password authentication mechanism.

TACACS+ Enable Password Attribute

The CLI EXEC mode is used for setting, viewing, and testing system operations. It is divided into two access levels, user and privileged. To access privileged-level EXEC mode, enter the enable EXEC command at the user access level prompt and specify a privileged EXEC password (superuser or admin-equivalent password) when prompted for a password.

In TACACS+, an enable password feature allows an administrator to define a different enable password per administrative-level user. If an administrative-level user logs in to the SE with a normal-level user account (privilege level of 0) instead of an admin or admin-equivalent user account (privilege level of 15), that user must enter the admin password in order to access privileged-level EXEC mode. This requirement applies even if these users are using TACACS+ for login authentication.

```
ServiceEngine> enable
Password:
```

Examples

The following example enables local and TACACS+ authentication and authorization, setting TACACS+ as the first method used and local as the secondary method to use if TACACS+ fails:

```
ServiceEngine(config)# authentication login tacacs enable primary
ServiceEngine(config)# authentication login local enable secondary
ServiceEngine(config)# authentication configuration local enable secondary
ServiceEngine(config)# authentication configuration tacacs enable primary
```

The following example shows the output of the show authentication user command:

```
ServiceEngine# show authentication user
Login Authentication: Console/Telnet Session
----------------------------- -----------------------
local enabled (secondary)
radius disabled
tacacs enabled (primary)
Configuration Authentication: Console/Telnet Session
----------------------------- -----------------------
local enabled (secondary)
radius disabled
tacacs enabled (primary)
Configuration Authentication: Console/Telnet Session
----------------------------- -----------------------
local enabled (secondary)
radius enabled (tertiary)
tacacs enabled (primary)
```

The following example shows the output of the **show authentication user** command:

```
ServiceEngine# show authentication user
Login Authentication: Console/Telnet/Ftp/SSH Session
----------------------------- ------------------------------
local disabled
Radius disabled
Tacacs+ disabled

Configuration Authentication: Console/Telnet/Ftp/SSH Session
----------------------------- ------------------------------
local disabled
Radius disabled
Tacacs+ disabled
```

The following example shows the output of the **show statistics authentication** command:

```
ServiceEngine# show statistics authentication
Authentication Statistics
--------------------------------------
Number of access requests: 37
Number of access deny responses: 14
Number of access allow responses: 23
```

The following example enables local, TACACS+, and RADIUS authentication and authorization, setting TACACS+ as the first method used, local as the secondary method if the TACACS+ method fails, and RADIUS as the tertiary method to use if both local and TACACS+ fail:

```
ServiceEngine(config)# authentication login tacacs enable primary
ServiceEngine(config)# authentication login local enable secondary
ServiceEngine(config)# authentication login radius enable tertiary
ServiceEngine(config)# authentication configuration tacacs enable primary
ServiceEngine(config)# authentication configuration local enable secondary
ServiceEngine(config)# authentication configuration radius enable tertiary
```

Related Commands

radius-server
show authentication
show statistics authentication
username

authsvr

To enable and configure the Authorization server, use the **authsvr** global configuration command. To disable the Authorization server, use the **no** form of this command.

authsvr {**enable** | **unknown-server allow**}

no authsvr {**enable** | **unknown-server allow**}

Syntax Description

enable	Enables the Authorization server.
unknown-server	Configures the Authorization server unknown server or domain.
allow	Allows requests for an unknown server or domain.

Defaults

authsvr: enabled

unknown-server: blocked

Command Modes

Global configuration

Examples

The following example shows how to enable the Authorization server:

```
ServiceEngine(config)#authsvr enable
Authserver is enabled
```

Related Commands

debug authsvr trace
debug authsvr error
debug authsvr
show statistics authsvr

bandwidth (global configuration)

To set an allowable bandwidth usage limit and its duration for Cisco Streaming Engine WMT streaming media, use the **bandwidth** global configuration command. To remove individual options, use the **no** form of this command.

bandwidth {**movie-streamer** {**incoming** *bandwidth* | **outgoing** *bandwidth* {**default** | **max-bandwidth start-time** *day hour* **end-time** *day hour*}} | **wmt** {**incoming** *bandwidth* | **outgoing** *bandwidth*}}

no bandwidth {**movie-streamer** {**incoming** *bandwidth* | **outgoing** *bandwidth* {**default** | **max-bandwidth start-time** *day hour* **end-time** *day hour*}} | **wmt** {**incoming** *bandwidth* | **outgoing** *bandwidth*}}

Syntax Description

movie-streamer	Configures the maximum pacing bit rate in kilobits per second (kbps) for the Movie Streamer.
incoming	Configures the duration of allowable incoming bandwidth settings for WMT.
bandwidth	Bandwidth size for the Movie Streamer in kilobits per second (kbps) (0–2147483647).
outgoing	Configures the duration of allowable outgoing bandwidth settings for WMT.
default	Specifies the default value for bandwidth if the scheduled bandwidth is not configured.
max-bandwidth	Specifies the maximum value of bandwidth in Kbps.
start-time	Specifies the start time for this bandwidth setting.
day	Day of the week.
hour	Time to start (hh:mm) (0–23:0–59)
end-time	Specifies the end time for this bandwidth setting.
wmt	Configures the duration of allowable bandwidth settings for WMT. For more information, see the "Configuring Incoming and Outgoing WMT Bandwidth" section on page 2-35.

Defaults

No default behavior or values.

Command Modes

Global configuration

Usage Guidelines

With the various types of traffic originating from a device, every type of traffic, such as streaming media, HTTP, and metadata, consumes network resources. Use the **bandwidth** command to limit the amount of network bandwidth used by the WMT streaming media.

The content services bandwidth includes the bandwidth allocation for WMT. WMT bandwidth settings apply to WMT streaming of live, cached, and pre-positioned content.

For each type of bandwidth, you can specify the amount of bandwidth to be used for a particular time period. This type is called *scheduled bandwidth*. The *default bandwidth* is the amount of bandwidth associated with each content service type when there is no scheduled bandwidth. In centrally managed deployments (the SEs are registered with a CDSM), if an SE is assigned to a device group and no default bandwidth has been configured for the SE itself, the device group default bandwidth settings are applied. However, if the default bandwidth has been configured for the SE, then that setting overrides the device group settings. If the SE is a member of multiple device groups, the most recently updated default bandwidth settings are applied.

The *maximum bandwidth* specifies the upper limit for the allowable bandwidth. The total bandwidth configured for all content services must not exceed the bandwidth limits specified for any SE platform model in the Internet Streamer CDS network. In addition, the license keys configured for WMT further restrict the maximum bandwidth available for each SE model.

Configuring Incoming and Outgoing WMT Bandwidth

The bandwidth between the WMT proxy server (the SE) and the WMT client is called the WMT outgoing bandwidth.

The bandwidth between the WMT proxy and the origin streaming server is called the incoming bandwidth. Because the bandwidth from the edge to the outside IP WAN is limited, you must specify a per session limit (the maximum bit rate per request) for each service that is running on the SE and that consumes the incoming bandwidth (for example, the WMT streaming service), and an aggregate limit (the maximum incoming bandwidth.) You need to control the outgoing bandwidth based on the WMT license that is configured on the SE.

The **bandwidth wmt outgoing** and **bandwidth incoming** global configuration commands enable you to specify a WMT incoming and an outgoing bandwidth as follows:

- Use the **bandwidth wmt outgoing** *kbits* global configuration command to specify the outgoing WMT bandwidth in kbps. This command sets the maximum bandwidth for the WMT content that can delivered to a client that is requesting WMT content. The range of values is between 0–2,147,483,647 kilobits per second (kbps).

  If the specified outgoing bandwidth is above the limit specified by the WMT license, then a warning message displays. However, the specified outgoing bandwidth setting is applied to the SE because the outgoing bandwidth may be configured before the WMT licenses are enabled or an enabled WMT license could be changed to a higher value at a later time.

- Use the **bandwidth wmt incoming** *kbits* global configuration command to specify the incoming WMT bandwidth in kbps. This command sets the maximum bandwidth for the WMT content that can delivered to an SE from the origin streaming server or another SE in the case of a cache miss. The specified bit rate is the maximum incoming WMT per session bit rate. The range of values is between 0–2,147,483,647 kbps. The incoming bandwidth applies to VoD content from the origin server for a cache miss.

Related Commands

bandwidth (interface configuration)
interface
show bandwidth
show interface
show running-config
show startup-config
show statistics bandwidth

bandwidth (interface configuration)

To configure an interface bandwidth, use the **bandwidth** interface configuration command. To restore default values, use the **no** form of this command.

bandwidth {**10** | **100** | **1000**}

no bandwidth {**10** | **100** | **1000**}

Syntax Description

10	Sets the bandwidth to 10 megabits per second (Mbps).
100	Sets the bandwidth to 100 Mbps.
1000	Sets the bandwidth to 1000 Mbps. This option is not available on all ports.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Usage Guidelines

To configure an interface bandwidth on an SE, use the **bandwidth** interface configuration command. The bandwidth is specified in megabits per second (Mbps). The **1000** Mbps option is not available on all ports. On a Service Engine model that has an optical Gigabit Ethernet interface, you cannot change the of this interface. Therefore, Gigabit Ethernet interfaces only run at 1000 Mbps. For newer models of the SE that have a Gigabit Ethernet interface over copper, this restriction does not apply; you can configure these Gigabit Ethernet interfaces to run at 10, 100, or 1000 Mbps.

You can configure the Gigabit Ethernet interface settings (bandwidth, and duplex settings) if the Gigabit-over-copper-interface is up or down. If the interface is up, it will apply the specific interface settings. If the interface is down, the specified settings are stored and then applied when the interface is brought up. For example, you can specify any of the following commands for a Gigabit-over-copper-interface, which is currently down, and have these settings automatically applied when the interface is brought up:

```
ServiceEngine(config-if)# bandwidth 10
ServiceEngine(config-if)# bandwidth 100
ServiceEngine(config-if)# bandwidth 1000
```

You cannot configure the Gigabit Ethernet interface settings on an optical Gigabit Ethernet interface.

Examples

The following example shows how to set an interface bandwidth to 10 Mbps:

```
ServiceEngine(config-if)#bandwidth 10
```

The following example shows how to restore default bandwidth values on an interface:

```
ServiceEngine(config-if)#no bandwidth
```

Related Commands

interface

banner

To configure the EXEC, login, and message-of-the-day (MOTD) banners, use the **banner** global configuration command. To disable the banner feature, use the **no** form of this command.

banner {**enable** | **exec** {**message** *line* | *message_text*} | **login** {**message** *line* | *message_text*} | **motd** {**message** *line* | *message_text*}}

no banner {**enable** | **exec** [**message**] | **login** [**message**] | **motd** [**message**]}

Syntax Description

enable	Enables banner support on the SE.
exec	Configures an EXEC banner.
message	Specifies a message to be displayed when an EXEC process is created.
line	EXEC message text on a single line. The SE translates the \n portion of the message to a new line when the EXEC banner is displayed to the user.
message_text	EXEC message text on one or more lines. Press the **Return** key or enter delimiting characters (\n) to specify an EXEC message to appear on a new line. Supports up to a maximum of 980 characters, including new-line characters (\n). Enter a period (.) at the beginning of a new line to save the message and return to the prompt for the global configuration mode. **Note** The EXEC banner content is obtained from the command line input that the user enters after being prompted for the input.
login	Configures a login banner.
message	Specifies a message to be displayed before the username and password login prompts.
line	Login message text on a single line. The SE translates the \n portion of the message to a new line when the login banner is displayed to the user.
message_text	Login message text on one or more lines. Press the **Return** key or enter delimiting characters (\n) to specify a login message to appear on a new line. Supports up to a maximum of 980 characters, including new-line characters (\n). Enter a period (.) at the beginning of a new-line to save the message and return to the prompt for the global configuration mode. **Note** The login banner content is obtained from the command line input that the user enters after being prompted for the input.
motd	Configures an MOTD banner.
message	Specifies an MOTD message.
line	MOTD message text on a single line. The SE translates the \n portion of the message to a new line when the MOTD banner is displayed to the user.
message_text	MOTD message text on one or more lines. Press the **Return** key or enter delimiting characters (\n) to specify an MOTD message to appear on a new line. Supports up to a maximum of 980 characters, including new-line characters (\n). Enter a period (.) at the beginning of a new line to save the message and return to the prompt for the global configuration mode. **Note** The MOTD banner content is obtained from the command line input that the user enters after being prompted for the input.

Defaults

Banner support is disabled by default

Command Modes

Global configuration

Usage Guidelines

You can configure the following three types of banners in any Internet Streamer CDS software device mode:

- The MOTD banner sets the message of the day. This message is the first message that is displayed when a login is attempted.
- The login banner is displayed after the MOTD banner but before the actual login prompt appears.
- The EXEC banner is displayed after the EXEC CLI shell has started.

Note All of these banners are effective on a console, Telnet, or a Secure Shell (SSH) version 2 session.

After you configure the banners, enter the **banner enable** global configuration command to enable banner support on the SE. Enter the **show banner** EXEC command to display information about the configured banners.

Note When you run an SSH version 1 client and log in to the SE, the MOTD and login banners are not displayed. You need to use SSH version 2 to display the banners when you log in to the SE.

Examples

The following example shows how to enable banner support on the SE:

```
ServiceEngine(config)# banner enable
```

The following example shows how to use the **banner motd message** global configuration command to configure the MOTD banner. In this example, the MOTD message consists of a single line of text.

```
ServiceEngine(config)# banner motd message This is an Internet Streamer CDS 2.3 device
```

The following example shows how to use the **banner motd message** global command to configure a MOTD message that is longer than a single line. In this case, the SE translates the \n portion of the message to a new line when the MOTD message is displayed to the user.

```
ServiceEngine(config)# banner motd message "This is the motd message.
\nThis is an Internet Streamer CDS 2.3 device\n"
```

The following example shows how to use the **banner login message** global configuration command to configure a MOTD message that is longer than a single line. In this case, SE A translates the \n portion of the message to a new line in the login message that is displayed to the user.

```
ServiceEngine(config)# banner login message "This is login banner.
\nUse your password to login\n"
```

The following example shows how to use the **banner exec** global configuration command to configure an interactive banner. The **banner exec** command is similar to the **banner motd message** commands except that for the **banner exec** command, the banner content is obtained from the command line input that the user enters after being prompted for the input.

```
ServiceEngine(config)#banner exec
```

```
Please type your MOTD messages below and end it with '.' at beginning of line:
(plain text only, no longer than 980 bytes including newline)
This is the EXEC banner.\nUse your Internet Streamer CDS username and password to log in
to this SE.\n
.
Message has 99 characters.
ServiceEngine(config)#
```

Assume that an SE has been configured with the MOTD, login, and EXEC banners as shown in the previous examples. When a user uses an SSH session to log in to the SE, the user will see a login session that includes a MOTD banner and a login banner that asks the user to enter a login password as follows:

```
This is the motd banner.
This is an Internet Streamer CDS 2.3 device
This is login banner.
Use your password to login.

Cisco SE

admin@ce's password:
```

After the user enters a valid login password, the EXEC banner is displayed, and the user is asked to enter the Internet Streamer CDS username and password as follows:

```
Last login: Fri Oct  1 14:54:03 2004 from client
System Initialization Finished.
This is the EXEC banner.
Use your Internet Streamer CDS username and password to log in to this SE.
```

After the user enters a valid Internet Streamer CDS username and password, the SE CLI is displayed. The CLI prompt varies depending on the privilege level of the login account. In the following example, because the user entered a username and password that had administrative privileges (privilege level of 15), the EXEC mode CLI prompt is displayed:

```
ServiceEngine#
```

Related Commands

show banner

bitrate

To configure the maximum pacing bit rate for large files for the Movie Streamer and to separately configure WMT bit-rate settings, use the **bitrate** global configuration command. To remove the bit-rate settings, use the **no** form of this command.

bitrate {**movie-streamer** *bitrate* | **wmt** {**incoming** *bitrate* | **outgoing** *bitrate*}}

no bitrate {**movie-streamer** *bitrate* | **wmt** {**incoming** | **outgoing**}}

Syntax Description

movie-streamer	Configures the maximum pacing bit rate in kilobits per second (kbps) for the Movie Streamer.
bitrate	Bit rate in kbps (1–2147483647).
wmt	Configures the bit rate, in kbps, for large files sent using the WMT protocol.
incoming	Sets the incoming bit-rate settings.
bitrate	Incoming bit rate in kbps (0–2147483647).
outgoing	Sets the outgoing bit-rate settings.
bitrate	Outgoing bit rate in kbps (0–2147483647).

Defaults

movie-streamer *bitrate*: 1500 kbps

wmt incoming *bitrate*: 0 (no limit)

wmt outgoing *bitrate*: 0 (no limit)

Command Modes

Global configuration

Usage Guidelines

The Internet Streamer CDS 2.x software includes the Windows Media Technologies (WMT) proxy, which has the ability to cache on-demand media files when the user requests these files for the first time. All subsequent requests for the same file are served by the WMT proxy using the RTSP protocol. The WMT proxy can also live-split a broadcast, which causes only a single unicast stream to be requested from the origin server in response to multiple client requests for the stream.

The bit rate between the proxy and the origin server is called the incoming bit rate. Use the **bitrate** command to limit the maximum bit rate per session for large files. The **bitrate wmt incoming** and **bitrate wmt outgoing** global configuration commands enable you to specify a WMT incoming and outgoing WMT per session bit rate as follows:

- Use the **bitrate wmt incoming** *bitrate* global configuration command to specify the maximum incoming streaming bit rate per session that can be delivered to the WMT proxy server (an SE) from the origin streaming server or another SE in the case of a cache miss. The specified bit rate is the maximum incoming WMT per session bit rate. The range of values is between 0–2,147,483,647 kbps. The default value is 0 (no bit-rate limit).

- Use the **bitrate wmt outgoing** *bitrate* global configuration command to set the maximum outgoing streaming bit rate per session that can delivered to a client that is requesting WMT content. The specified bit rate is the maximum outgoing WMT per session bit rate). The range of values is between 0–2,147,483,647 kbps. The default value is 0 (no bit-rate limit). The outgoing bandwidth applies to VoD content from the WMT proxy server on the SE in the case of a cache miss.

Note The aggregate bandwidth used by all concurrent users is still limited by the default device bandwidth or by the limit configured using the **bandwidth** global configuration command.

Variable WMT Bit Rates

A content provider can create streaming media files at different bit rates to ensure that different clients who have different connections—for example, modem, DSL, or LAN—can choose a particular bit rate. The WMT caching proxy can cache multiple bit-rate files or variable bit-rate (VBR) files, and based on the bit rate specified by the client, it serves the appropriate stream. Another advantage of creating variable bit-rate files is that you only need to specify a single URL for the delivery of streaming media.

Note In the case of multiple bit-rate files, the SE that is acting as the WMT proxy server only retrieves the bit rate that the client has requested.

Examples

The following example shows how to configure an incoming bit rate for the Movie Streamer:

```
ServiceEngine(config)#bitrate movie-streamer incoming 100
```

The following example shows how to configure an incoming bit rate for a file sent using WMT. Use the **show wmt** command to verify that the incoming bit rate has been modified.

```
ServiceEngine(config)#bitrate wmt incoming 300000
ServiceEngine(config)#exit
ServiceEngine#show wmt
--------- WMT Server Configurations -----------------
WMT is enabled
WMT disallowed client protocols: none
WMT bandwidth platform limit: 1000000 Kbits/sec
WMT outgoing bandwidth configured is 500000 Kbits/sec
WMT incoming bandwidth configured is 500000 Kbits/sec
WMT max sessions configured: 14000
WMT max sessions platform limit: 14000
WMT max sessions enforced: 14000 sessions
WMT max outgoing bit rate allowed per stream has no limit
WMT max incoming bit rate allowed per stream has no limit
WMT cache is enabled
WMT cache max-obj-size: 25600 MB
WMT cache revalidate for each request is not enabled
WMT cache age-multiplier: 30%
WMT cache min-ttl: 60 minutes
WMT cache max-ttl: 1 days
WMT debug client ip not set
WMT debug server ip not set
WMT accelerate live-split is enabled
WMT accelerate proxy-cache is enabled
WMT accelerate VOD is enabled
WMT fast-start is enabled
WMT fast-start max. bandwidth per player is 3500 (Kbps)
WMT fast-cache is enabled
WMT fast-cache acceleration factor is 5
WMT maximum data packet MTU (TCP) enforced is 1472 bytes
WMT maximum data packet MTU (UDP) is 1500 bytes
WMT client idle timeout is 60 seconds
WMT forward logs is enabled
WMT server inactivity-timeout is 65535
WMT Transaction Log format is Windows Media Services 4.1 logging
RTSP Gateway incoming port 554

--------- WMT HTTP Configurations -------------------
WMT http extensions allowed:
asf none nsc wma wmv nsclog

--------- WMT Proxy Configurations ------------------
Outgoing Proxy-Mode:
--------------------
MMS-over-HTTP Proxy-Mode:
is not configured.
RTSP Proxy-Mode:
is not configured. ServiceEngine#
```

Related Commands

show wmt

cache

To restrict the maximum number of contents in the CDS, use the **cache** global configuration command.

cache content max-cached-entries *num*

Syntax Description

content	Browses the cdnfs directories and files.
max-cached-entries	Cleans up the unwanted entries in the cdnfs.
num	Max cached entries (1–10000000).

Defaults

The max-cached-entries default is 3000000 entries.

Command Modes

Global configuration

Usage Guidelines

The **cache** command configures the cached content maximum entries. The CDS, by default, allows a maximum of three million cached entries, regardless of the amount of space available in the cdnfs.

Examples

The following example shows how to configure the cache content:

```
ServiceEngine#cache content max-cached-entries 1000
```

Related Commands

show cache

capability

To modify the capability configuration, use the **capability** global configuration command. To disable capability, use the **no** form of this command.

capability config profile *number* [**add attrib** {**capability-url** *url* | **user-agent** *name*} | **description**]

no capability config

Syntax Description

config	Enters the capability exchange submode.
profile	Populates the profile database.
number	The profile ID (1–65535).
add	(Optional) Adds the capability attributes.
attrib	Adds the capability attributes.
capability-url	Specifies the capability URL.
url	The capability URL string.
user-agent	Specifies the user-agent.
name	The user-agent name.
description	(Optional) Specifies the profile description.

Defaults

No default behavior or values.

Command Modes

Global configuration

Related Commands

show capability

cd

To change from one directory to another directory, use the **cd** EXEC command.

cd *directoryname*

Syntax Description

directoryname	Directory name.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Use this command to maneuver between directories and for file management. The directory name becomes the default prefix for all relative paths. Relative paths do not begin with a slash (/). Absolute paths begin with a slash (/).

Examples

The following example shows how to use a relative path:

```
ServiceEngine(config)#cd local1
```

The following example shows how to use an absolute path:

```
ServiceEngine(config)#cd /local1
```

Related Commands

deltree
dir
lls
ls
mkdir
pwd

cdnfs

To manage the Internet Streamer CDS network file system (cdnfs), use the **cdnfs** EXEC command.

cdnfs {**browse** | **cleanup** {**info** | **start** {**force**} | **stop**}}

Syntax Description

browse	Browses the cdnfs directories and files.
cleanup	Cleans up the unwanted entries in the cdnfs.
info	Summarizes the information about unwanted entries without starting the cleanup process.
start	Starts the cleanup of unwanted entries in the cdnfs.
force	Removes objects that are in transient states.
stop	Stops the cleanup of unwanted entries in the cdnfs.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

The Internet Streamer CDS network file systems (cdnfs) stores the pre-positioned Internet Streamer CDS network content to be delivered by all supported protocols. You can configure the cdnfs size of each SE using the **disk configure** command.

The **cdnfs cleanup** command cleans up the content of deleted channels from the acquisition and distribution database. In certain cases, the acquirer is not notified by the Centralized Management System (CMS) about deleted channels, and it fails to clear all unified name space (UNS) content. In such cases, the **cdnfs cleanup** EXEC command can be used to clean up all UNS content associated with deleted channels.

Note You can use the **cdnfs cleanup start** to clean up the orphan content. The orphan content is content that is not associated with any channel to which an SE is subscribed.

The **cdnfs browse** command is an interactive command and has the following subcommands used to view Internet Streamer CDS network files and directories:

```
ServiceEngine#cdnfs browse

------  CDNFS interactive browsing  ------
dir, ls:   list directory contents
cd,chdir:  change current working directory
info:      display attributes of a file
more:      page through a file
cat:       display a file
exit,quit: quit CDNFS browse shell

/>dir
                    www.gidtest.com/
/>cd www.gidtest.com
```

```
/www.gidtest.com/>dir
764 Bytes           index.html
/www.gidtest.com/>info index.html

CDNFS File Attributes:
  Status                 3  (Ready)
  File Size              764 Bytes
  Start Time             null
  End Time               null
  Last-modified Time     Sun Sep  9 01:46:40 2001

Internal path to data file:
/disk06-00/d/www.gidtest.com/05/05d201b7ca6fdd41d491eaec7cfc6f14.0.data.html
  note: data file actual last-modified time: Tue Feb 15 00:47:35 2005

/www.gidtest.com/>
```

Because the cdnfs is empty in this example, the **ls** command does not show any results. Typically, if the cdnfs contained information, it would list the websites as directories, and file attributes and content could be viewed using these subcommands.

The **cdnfs cleanup** command synchronizes the state of the acquisition and distribution database with the content stored on the cdnfs. You should use this command after replacing a failed disk drive.

Examples

The following example shows the output of the **cdnfs cleanup info** command:

```
ServiceEngine#cdnfs cleanup info
Gathering cleanup information. This may take some time....
(Use Ctrl+C or 'cdnfs cleanup stop' to interrupt)
..............................

Summary of garbage resource entries found
-------------------------------------------
Number of entries    : 605
Size of entries (KB) : 60820911
```

Related Commands

show cdnfs
show statistics cdnfs

cdsm

To configure the Content Delivery System (CDSM) IP address to be used for the SEs or SRs, or to configure the role and GUI parameters on a CDSM device, use the **cdsm** global configuration command. To negate these actions, use the **no** form of this command.

cdsm {**ip** {*hostname* | *ip-address* | **role** {**primary** | **standby**} | **ui port** *port-num*}}

no cdsm {**ip** | **role** {**primary** | **standby**} | **ui port**}

Syntax Description

ip	Configures the CDSM hostname or IP address.
hostname	Hostname of the CDSM.
ip-address	IP address of the CDSM.
role	Configures the CDSM role to either primary or standby (available from the CDSM CLI only).
primary	Configures the CDSM to be the primary CDSM.
standby	Configures the CDSM to be the standby CDSM.
ui	Configures the CDSM GUI port address (available from the CDSM CLI only).
port	Configures the CDSM GUI port.
port-num	Port number (1–65535).

Defaults

No default behavior or values.

Command Modes

Global configuration

Usage Guidelines

You can use the **cdsm ui port** global configuration command to change the CDSM GUI port from the standard number 8443 as follows:

```
CDSM(config)#cdsm ui port 35535
```

Note The **role** and **ui** options are available on CDSM devices only. Changing the CDSM GUI port number automatically restarts the Centralized Management System (CMS) service if this has been enabled.

The **cdsm ip** command associates the device with the CDSM so that the device can be approved as a part of the network.

After the device is configured with the CDSM IP address, it presents a self-signed security certificate and other essential information, such as its IP address or hostname, disk space allocation, and so forth, to the CDSM.

Configuring Devices Inside a NAT

In an Internet Streamer CDS network, there are two methods for a device registered with the CDSM (SEs, SRs, or standby CDSM) to obtain configuration information from the primary CDSM. The primary method is for the device to periodically poll the primary CDSM on port 443 to request a configuration update. You cannot configure this port number. The backup method is when the CDSM pushes configuration updates to a registered device as soon as possible by issuing a notification to the registered device on port 443. This method allows changes to take effect in a timelier manner. You cannot configure this port number even when the backup method is being used. Internet Streamer CDS networks do not work reliably if devices registered with the CDSM are unable to poll the CDSM for configuration updates. Similarly, when a receiver SE requests content and content metadata from a forwarder SE, it contacts the forwarder SE on port 443.

All the above methods become complex in the presence of Network Address Translation (NAT) firewalls. When a device (SEs at the edge of the network, SRs, and primary or standby CDSMs) is inside a NAT firewall, those devices that are inside the same NAT use one IP address (the inside local IP address) to access the device and those devices that are outside the NAT use a different IP address (the inside global IP address) to access the device. A centrally managed device advertises only its inside local IP address to the CDSM. All other devices inside the NAT use the inside local IP address to contact the centrally managed device that resides inside the NAT. A device that is not inside the same NAT as the centrally managed device is not able to contact it without special configuration.

If the primary CDSM is inside a NAT, you can allow a device outside the NAT to poll it for getUpdate requests by configuring a *static translation* (inside global IP address) for the CDSM's inside local IP address on its NAT, and using this address, rather than the CDSM's inside local IP address, in the **cdsm ip** *ip-address* global configuration command when you register the device to the CDSM. If an SE or SR is inside a NAT and the CDSM is outside the NAT, you can allow the SE or SR to poll for getUpdate requests by configuring a static translation (inside global IP address) for the SE or SIR's inside local address on its NAT and specifying this address in the Use IP Address field under the NAT Configuration heading in the Device Activation window.

Note Static translation establishes a one-to-one mapping between your inside local address and an inside global address. Static translation is useful when a host on the inside must be accessible by a fixed address from the outside.

Standby CDSMs

The Cisco Internet Streamer CDS software implements a standby CDSM. This process allows you to maintain a copy of the Internet Streamer CDS network configuration. If the primary CDSM fails, the standby can be used to replace the primary.

For interoperability, when a standby CDSM is used, it must be at the same software version as the primary CDSM in order to maintain the full CDSM configuration. Otherwise, the standby CDSM detects this status and does not process any configuration updates that it receives from the primary CDSM until the problem is corrected.

Note We recommend that you upgrade your standby CDSM first and then upgrade your primary CDSM. We also recommend that you create a database backup on your primary CDSM and copy the database backup file to a safe place before you upgrade the software.

Switching a CDSM from Warm Standby to Primary

If your primary CDSM becomes inoperable for some reason, you can manually reconfigure one of your warm standby CDSMs to be the primary CDSM. Configure the new role by using the global configuration **cdsm role primary** command as follows:

```
ServiceEngine#configure
ServiceEngine(config)#cdsm role primary
```

This command changes the role from standby to primary and restarts the management service to recognize the change.

Note Check the status of recent updates from the primary CDSM. Use the **show cms info** EXEC command and check the time of the last update. To be current, the update time should be between 1 and 5 minutes old. You are verifying that the standby CDSM has fully replicated the primary CDSM configuration. If the update time is not current, check whether there is a connectivity problem or if the primary CDSM is down. Fix the problem, if necessary, and wait until the configuration has replicated as indicated by the time of the last update. Make sure that both CDSMs have the same Coordinated Universal Time (UTC) configured.

If you switch a warm standby CDSM to primary while your primary CDSM is still online and active, both CDSMs detect each other, automatically shut themselves down, and disable management services. The CDSMs are switched to halted, which is automatically saved in flash memory.

Examples

The following example configures an IP address and a primary role for a CDSM:

```
CDSM(config)#cdsm ip 10.1.1.1
CDSM(config)#cdsm role primary
```

The following example configures a new GUI port to access the CDSM GUI:

```
CDSM(config)#cdsm ui port 8550
```

The following example configures the CDSM as the standby CDSM:

```
CDSM(config)#cdsm role standby
Switching CDSM to standby will cause all configuration settings made on this CDSM
 to be lost.
Please confirm you want to continue [no]?yes
Restarting CMS services
```

The following example configures the standby CDSM with the IP address of the primary CDSM by using the **cdsm ip** *ip-address* global configuration command. This command associates the device with the primary CDSM so that it can be approved as a part of the network.

```
CDSM# cdsm ip 10.1.1.1
```

clear

To clear the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings, use the **clear** EXEC command.

On the SE:

clear cache [**all** | **content** *1-1000000* | **flash-media-streaming**]

clear content url *url*

clear ip access-list counters [*acl-num* | *acl-name*]

clear logging

clear statistics {**access-lists 300** | **all** | **authentication** | **authsvr** | **distribution** {**all** | **metadata-receiver** | **metadata-sender** | **unicast-data-receiver** | **unicast-data-sender**} | **flash-media-streaming** | **history** | **http** {**all** | **ims** | **object** | **pcmm** | **performance** | **requests** | **rule**} | **icap** | **icmp** | **ip** | **movie-streamer** | **qos policy-service** | **radius** | **rule** {**action** *action-type* | **all** | **pattern** {**1-512** | **all**} | **rtsp**} | **running** | **snmp** | **tacacs** | **tcp** | **transaction-logs** | **udp** | **wmt**}

clear transaction-log

clear users administrative

clear wmt stream-id *1-999999*

On the SR:

clear ip access-list counters [*acl-num* | *acl-name*]

clear logging

clear statistics {**all** | **authentication** | **history** | **http** {**all** | **ims** | **object** | **pcmm** | **performance** | **requests** | **rule**} | **icmp** | **ip** | **radius** | **running** | **service-router** | **snmp** | **tacacs** | **tcp** | **udp**}

clear users administrative

On the CDSM:

clear ip access-list counters [*acl-num* | *acl-name*]

clear logging

clear statistics {**all** | **authentication** | **distribution** {**all** | **metadata-receiver** | **metadata-sender** | **unicast-data-receiver** | **unicast-data-sender**} | **history** | **icmp** | **ip** | **radius** | **running** | **snmp** | **tacacs** | **tcp** | **udp**}

clear users administrative

Syntax Description

cache	Clears the HTTP objects from the cache.
all	(Optional) Clears all cached objects.
content	(Optional) Clears cached content.

1-1000000	Free space in MBs.
flash-media-streaming	Clears the Flash Media Streaming edge server cached content and DVR cached content.
content	Clears all cached content.
url	Clears cached content with its original URL.
url	The URL for the content object to delete.
ip access-list	Clears the IP access list statistical information.
counters	Clears the IP access list counters.
acl-name	(Optional) Counters for the specified access list, identified using an alphanumeric identifier up to 30 characters, beginning with a letter.
acl-num	(Optional) Counters for the specified access list, identified using a numeric identifier (standard access list: 1–99; extended access list: 100–199).
logging	Clears the syslog messages saved in the disk file.
statistics	Clears the statistics as specified.
access-lists	Clears the access control list statistics.
300	Clears the group name-based access control list.
all	Clears all statistics.
authentication	Clears the authentication statistics.
authsvr	Clears the Authorization Server statistics.
distribution	Clears the distribution statistics.
all	Clears the distribution statistics for every component.
metadata-receiver	Clears the distribution statistics for the metadata receiver.
metadata-sender	Clears the distribution statistics for the metadata sender.
unicast-data-receiver	Clears the distribution statistics for the unicast data receiver.
unicast-data-sender	Clears the distribution statistics for the unicast data sender.
flash-media-streaming	Clears the Flash Media Streaming statistics.
history	Clears the statistics history.
http	Clears the cache containing HTTP and FTP objects.
all	(Optional) Clears all HTTP statistics.
ims	(Optional) Clears the HTTP if-modified-since (IMS) statistics.
object	(Optional) Clears the HTTP object statistics.
pcmm	(Optional) Clears the HTTP PCMM statistics.
performance	(Optional) Clears the HTTP performance statistics.
requests	(Optional) Clears the nontunneled HTTPS request statistics.
rule	(Optional) Clears the HTTP rule statistics.
icap	Clears the ICAP statistics.
icmp	Clears the ICMP statistics.
ip	Clears the IP statistics.
movie-streamer	Clears the Movie Streamer statistics.
qos	Clears the QoS statistics.
policy-service	Specifies the Camiant cdn-am service.

radius	Clears the RADIUS statistics.
rule	Clears the rules statistics.
action	Clears the statistics of all the rules with the same action.
action-type	Specifies one of the following actions: **allow** **append-username-header** **block** **cache-non-cacheable** **cache-only** **dscp client cache-hit** **dscp client cache-miss** **dscp server** **freshness-factor** **insert-no-cache** **no-auth** **no-cache** **no-persistent-connection** **no-proxy** **no-url-filtering** **redirect** **redirect-url-for-cdn** **refresh** **reset** **rewrite** **use-icap-service** **use-proxy** **use-proxy failover** **use-server** **use-xforward-clt-ip**
all	Clears the statistics of all the rules.
pattern	Clears the statistics of the pattern lists.
1-512	Pattern list number.
all	Clears the statistics for all the pattern lists.
rtsp	Clears the statistics for the configured RTSP rules (rules configured for RTSP requests from RealMedia players [the RTSP rules] and rules configured for RTSP requests from Windows Media 9 players [the WMT-RTSP rules]).
running	Clears the running statistics.
snmp	Clears the SNMP statistics.
tacacs	Clears the TACACS+ statistics.
tcp	Clears the TCP statistics.
transaction-logs	Clears the transaction log export statistics.
udp	Clears the UDP statistics.
wmt	Clears all WMT statistics.
transaction-log	Archives the working transaction log files.
users	Clears the connections (login) of authenticated users.

administrative	Clears the connections of administrative users authenticated through a remote login service.
wmt	Clears the WMT streams.
stream-id	Clears the WMT streams that have the specified WMT stream ID. Also stops the SE's WMT process that is associated with the specified stream ID.
1-999999	WMT stream ID to clear.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

The **clear cache** command removes all cached contents from the currently mounted cache volumes. Objects being read or written are removed when they stop being busy. The equivalent to this command is the **cache clear** command.

Caution This command is irreversible, and all cached content will be erased.

The **clear cache force** command deletes all objects, whether busy or not, and may generate broken GIF or HTML messages for objects that were being read from the disk when the command was executed.

The **clear logging** command removes all current entries from the syslog.txt file, but does not make an archive of the file. It puts a "Syslog cleared" message in the syslog.txt file to indicate that the syslog has been cleared, as shown in the following example:

```
Feb 14 12:17:18 ServiceEngine#exec_clear_logging:Syslog cleared
```

The **clear statistics** command clears all statistical counters from the parameters given. Use this command to monitor fresh statistical data for some or all features without losing cached objects or configurations.

The **clear transaction-log** command causes the transaction log to be archived immediately to the SE hard disk. This command has the same effect as the **transaction-log force archive** command.

The **clear users administrative** command clears the connections for all administrative users who are authenticated through a remote login service, such as TACACS. This command does not affect an administrative user who is authenticated through the local database.

Examples

The following example shows that the **clear transaction-log** option forces the working transaction log file to be archived:

```
ServiceEngine#clear transaction-log
```

Related Commands

cache clear
show interface
show statistics

clock (EXEC)

To set or clear clock functions or update the calendar, use the **clock** EXEC command.

clock {**read-calendar** | **set** *time day month year* | **update-calendar**}

Syntax Description

read-calendar	Reads the calendar and updates the system clock.
set	Sets the time and date.
time	Current time in hh:mm:ss format (hh: 00–23; mm: 00–59; ss: 00–59).
day	Day of the month (1–31).
month	Month of the year (January, February, March, April, May, June, July, August, September, October, November, December).
year	Year (1993–2035).
update-calendar	Updates the calendar with the system clock.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

If you have an outside source on your network that provides time services (such as a Network Time Protocol [NTP] server), you do not need to set the system clock manually. When setting the clock, enter the local time. The SE calculates the Coordinated Universal Time (UTC) based on the time zone set by the **clock timezone** global configuration command.

Note We strongly recommend that you configure the SE for the Network Time Protocol (NTP) by using the **ntp** global configuration command. See the "ntp" section on page -161 for more details.

Two clocks exist in the system: the software clock and the hardware clock. The software uses the software clock. The hardware clock is used only at bootup to initialize the software clock. The calendar clock is the same as the hardware clock that runs continuously on the system, even if the system is powered off or rebooted. This clock is separate from the software clock settings, which are erased when the system is powered cycled or rebooted.

The **set** keyword sets the software clock. If the system is synchronized by a valid outside timing mechanism, such as a Network Time Protocol (NTP) clock source, you do not need to set the system clock. Use this command if no other time sources are available. The time specified in this command is relative to the configured time zone.

To perform a one-time update of the hardware clock (calendar) from the software clock or to copy the software clock settings to the hardware clock (calendar), use the **clock update-calendar** EXEC command.

Examples

The following example sets the software clock on the SE:

```
ServiceEngine#clock set 13:32:00 01 February 2000
```

Related Commands

clock timezone
ntp
show clock detail

clock (global configuration)

To set the summer daylight saving time and time zone for display purposes, use the **clock** global configuration command. To disable this function, use the **no** form of this command.

```
clock {summertime timezone {date startday startmonth startyear starthour endday endmonth
    endyear offset | recurring {1-4 startweekday startmonth starthour endweekday endmonth
    endhour offset | first startweekday startmonth starthour endweekday endmonth endhour
    offset | last startweekday startmonth starthour endweekday endmonth endhour offset}} |
    timezone {timezone hoursoffset minutesoffset}}

no clock {summertime timezone {date startday startmonth startyear starthour endday endmonth
    endyear offset | recurring {1-4 startweekday startmonth starthour endweekday endmonth
    endhour offset | first startweekday startmonth starthour endweekday endmonth endhour
    offset | last startweekday startmonth starthour endweekday endmonth endhour offset}} |
    timezone {timezone hoursoffset minutesoffset}}
```

Syntax Description

summertime	Configures the summer or daylight saving time.
timezone	Name of the summer time zone.
date	Configures the absolute summer time.
startday	Date (1–31) to start.
startmonth	Month (January through December) to start.
startyear	Year (1993–2032) to start.
starthour	Hour (0–23) to start in (hh:mm) format.
endday	Date (1–31) to end.
endmonth	Month (January through December) to end.
endyear	Year (1993–2032) to end.
endhour	Hour (0–23) to end in (hh:mm) format.
offset	Minutes offset (see Table B-1 on page B-1) from Coordinated Universal Time (UTC) (0–59).
recurring	Configures the recurring summer time.
1-4	Configures the starting week number 1–4.
first	Configures the summer time to recur beginning the first week of the month.
last	Configures the summer time to recur beginning the last week of the month.
startweekday	Day of the week (Monday–Friday) to start.
startmonth	Month (January–December) to start.
starthour	Hour (0–23) to start in (hh:mm) format.
endweekday	Weekday (Monday–Friday) to end.
endmonth	Month (January–December) to end.
endhour	Hour (0–23) to end in hour:minute (hh:mm) format.
offset	Minutes offset (see Table B-1 on page B-1) from UTC (0–59).
timezone	Configures the standard time zone.
timezone	Name of the time zone.

hoursoffset	Hours offset (see Table B-1 on page B-1) from UTC (–23 to +23).
minutesoffset	Minutes offset (see Table B-1 on page B-1) from UTC (0–59).

Defaults

No default behavior or values.

Command Modes

Global configuration

Usage Guidelines

To set and display the local and UTC current time of day without an NTP server, use the **clock timezone** command with the **clock set** command. The **clock timezone** parameter specifies the difference between UTC and local time, which is set with the **clock set** EXEC command. The UTC and local time are displayed with the **show clock detail** EXEC command.

Use the **clock** *timezone offset* command to specify a time zone, where *timezone* is the desired time zone entry from Table B-1 on page B-1 and *0 0* is the offset (ahead or behind) Coordinated Universal Time (UTC) in hours and minutes. UTC was formerly known as Greenwich mean time (GMT).

```
SE(config)#clock timezone timezone 0 0
```

Note The time zone entry is case sensitive and must be specified in the exact notation listed in the time zone table as shown in Appendix B, "Standard Time Zones." When you use a time zone entry from Table B-1 on page B-1, the system is automatically adjusted for daylight saving time.

The offset (ahead or behind) UTC in hours, as displayed in Table B-1 on page B-1, is in effect during winter time. During summer time or daylight saving time, the offset may be different from the values in the table and are calculated and displayed accordingly by the system clock.

Note An accurate clock and timezone setting is required for the correct operation of the HTTP proxy caches.

Examples

The following example specifies the local time zone as Pacific Standard Time with an offset of 8 hours behind UTC:

```
ServiceEngine(config)#clock timezone PST -8
Custom Timezone: PST will be used.
```

The following example configures a standard time zone on the SE:

```
ServiceEngine(config)#clock timezone US/Pacific 0 0
Resetting offset from 0 hour(s) 0 minute(s) to -8 hour(s) 0 minute(s)
Standard Timezone: US/Pacific will be used.
ServiceEngine(config)#
```

The following example negates the time zone setting on the SE:

```
ServiceEngine(config)#no clock timezone
```

The following example configures daylight saving time:

```
ServiceEngine(config)#clock summertime PDT date 10 October 2001 23:59 29 April 2002 23:59
60
```

Related Commands

clock
show clock detail

cms (EXEC)

To configure the Centralized Management System (CMS) embedded database parameters, use the **cms** EXEC command.

cms {**config-sync** | **database** {**backup** | **create** | **delete** | **downgrade** [**script** *filename*] | **maintenance** {**full** | **regular**} | **restore** *filename* | **validate**} | **deregister** [**force**] | **recover** {**identity** *word*}}

Syntax Description

config-sync	Sets the node to synchronize configuration with the CDSM.
database	Creates, backs up, deletes, restores, or validates the CMS-embedded database management tables or files.
backup	Backs up the database management tables.
create	Creates the embedded database management tables.
delete	Deletes the embedded database files.
downgrade	Downgrades the CMS database.
script	(Optional) Downgrades the CMS database by applying a downgrade script.
filename	Downgraded script filename.
maintenance	Cleans and reindexes the embedded database tables.
full	Specifies a full maintenance routine for the embedded database tables.
regular	Specifies a regular maintenance routine for the embedded database tables.
restore	Restores the database management tables using the backup local filename.
filename	Database local backup filename.
validate	Validates the database files.
deregister	Removes the registration of the CMS proto device.
force	(Optional) Forces the removal of the node registration.
recover	Recovers the identity of an CDS network device.
identity	Specifies the identity of the recovered device.
word	Identity of the recovered device.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

The CDS network is a collection of SR, SE, and CDSM nodes. One primary CDSM retains the CDS network settings and provides other CDS network nodes with updates. Communication between nodes occurs over secure channels using the Secure Shell Layer (SSL) protocol, where each node on the CDS network uses a Rivest, Shamir, Adelman (RSA) certificate-key pair to communicate with other nodes.

Use the **cms config-sync** command to enable registered SRs, SEs, and standby CDSM to contact the primary CDSM immediately for a getUpdate (get configuration poll) request before the default polling interval of 5 minutes. For example, when a node is registered with the primary CDSM and activated, it appears as Pending in the CDSM GUI until it sends a getUpdate request. The **cms config-sync** command causes the registered node to send a getUpdate request at once, and the status of the node changes as Online.

Use the **cms database create** command to initialize the CMS database. Before a node can join an CDS network, it must first be registered and then activated. The **cms enable** global configuration command automatically registers the node in the database management tables and enables the CMS. The node sends its attribute information to the CDSM over the SSL protocol and then stores the new node information. The CDSM accepts these node registration requests without admission control and replies with registration confirmation and other pertinent security information required for getting updates. Activate the node using the CDSM GUI.

Once the node is activated, it automatically receives configuration updates and the necessary security RSA certificate-key pair from the CDSM. This security key allows the node to communicate with any other node in the CDS network. The **cms deregister** command removes the node from the CDS network by deleting registration information and database tables.

To back up the existing management database for the CDSM, use the **cms database backup** command. For database backups, specify the following items:

- Location, password, and user ID
- Dump format in PostgreSQL plain text syntax

The naming convention for backup files includes the time stamp.

When you use the **cms recover identity** *word* command when recovering lost registration information, or replacing a failed node with a new node that has the same registration information, you must specify the device recovery key that you configured in the Modifying Config Property, System.device.recovery.key window of the CDSM GUI.

Use the **lcm** command to configure local/central management (LCM) on an CDS network device. The LCM feature allows settings configured using the device CLI or GUI to be stored as part of the CDS network-wide configuration data (enable or disable).

When you enter the **cms lcm enable** command, the CMS process running on SEs, SRs, and the standby CDSM detects the configuration changes that you made on these devices using CLIs and sends the changes to the primary CDSM.

When you enter the **cms lcm disable** command, the CMS process running on SEs, SRs, and the standby CDSM does not send the CLI changes to the primary CDSM. Settings configured using the device CLIs will not be sent to the primary CDSM.

If LCM is disabled, the settings configured through the CDSM GUI will overwrite the settings configured from the SE or SR; however, this rule applies only to those local device settings that have been overwritten by the CDSM when you have configured the local device settings. If you (as the local CLI user) change the local device settings after the particular configuration has been overwritten by the CDSM, the local device configuration will be applicable until the CDSM requests a full device statistics update from the SE or SR (clicking the **Force full database update** button from the Device Home window of the CDSM GUI triggers a full update). When the CDSM requests a full update from the device, the CDSM settings will overwrite the local device settings.

Examples

The following example backs up the database management tables:

```
CDSM# cms database backup
creating backup file with label `backup'
backup file local1/CDS-db-9-22-2002-17-36.dump is ready. use `copy' commands to move the
backup file to a remote host.
```

The following example validates the database management tables:

```
CDSM# cms database validate
Management tables are valid
```

In the following example, the CMS deregistration process has problems deregistering the SE, but it proceeds to deregister it from the CMS database when the **force** option is used:

```
ServiceEngine#cms deregister force
Deregistration requires management service to be stopped.
You will have to manually start it. Stopping management service on this node...
This operation needs to restart http proxy and streaming proxies/servers (if running) for
memory reconfiguration. Proceed? [no]yes
management services stopped
Thu Jun 26 13:17:34 UTC 2003 [I] main: creating 24 messages
Thu Jun 26 13:17:34 UTC 2003 [I] main: creating 12 dispatchers
Thu Jun 26 13:17:34 UTC 2003 [I] main: sending eDeRegistration message to CDSM
10.107.192.168
...
ServiceEngine#
```

The following example shows the use of the **cms recover identity** command when the recovery request matches the SE record, and the CDSM updates the existing record and sends a registration response to the requesting SE:

```
ServiceEngine#cms recover identity default
Registering this node as Service Engine...
Sending identity recovery request with key default
Thu Jun 26 12:54:42 UTC 2003 [I] main: creating 24 messages
Thu Jun 26 12:54:42 UTC 2003 [I] main: creating 12 dispatchers
Thu Jun 26 12:54:42 UTC 2003 [I] main: Sending registration message to CDSM
10.107.192.168
Thu Jun 26 12:54:44 UTC 2003 [W] main: Unable to load device info file in TestServer
Thu Jun 26 12:54:44 UTC 2003 [I] main: Connecting storeSetup for SE.
Thu Jun 26 12:54:44 UTC 2003 [I] main: Instantiating AStore
'com.cisco.unicorn.schema.PSqlStore'...
Thu Jun 26 12:54:45 UTC 2003 [I] main: Successfully connected to database
Thu Jun 26 12:54:45 UTC 2003 [I] main: Registering object factories for persistent
store...
Thu Jun 26 12:54:51 UTC 2003 [I] main: Dropped Sequence IDSET.
Thu Jun 26 12:54:51 UTC 2003 [I] main: Successfully removed old management tables
Thu Jun 26 12:54:51 UTC 2003 [I] main: Registering object factories for persistent
store...
.
.
.
Thu Jun 26 12:54:54 UTC 2003 [I] main: Created Table FILE_CDSM.
Thu Jun 26 12:54:55 UTC 2003 [I] main: Created SYS_MESS_TIME_IDX index.
Thu Jun 26 12:54:55 UTC 2003 [I] main: Created SYS_MESS_NODE_IDX index.
Thu Jun 26 12:54:55 UTC 2003 [I] main: No Consistency check for store.
Thu Jun 26 12:54:55 UTC 2003 [I] main: Successfully created management tables
Thu Jun 26 12:54:55 UTC 2003 [I] main: Registering object factories for persistent
store...
Thu Jun 26 12:54:55 UTC 2003 [I] main: AStore Loading store data...
Thu Jun 26 12:54:56 UTC 2003 [I] main: ExtExpiresRecord Loaded 0 Expires records.
Thu Jun 26 12:54:56 UTC 2003 [I] main: Skipping Construction RdToClusterMappings on
non-CDSM node.
Thu Jun 26 12:54:56 UTC 2003 [I] main: AStore Done Loading. 327
Thu Jun 26 12:54:56 UTC 2003 [I] main: Created SYS_MESS_TIME_IDX index.
Thu Jun 26 12:54:56 UTC 2003 [I] main: Created SYS_MESS_NODE_IDX index.
Thu Jun 26 12:54:56 UTC 2003 [I] main: No Consistency check for store.
Thu Jun 26 12:54:56 UTC 2003 [I] main: Successfully initialized management tables
Node successfully registered with id 103
Registration complete.
```

```
ServiceEngine#
```

The following example shows the use of the **cms recover identity** command when the hostname of the SE does not match the hostname configured in the CDSM graphical user interface:

```
ServiceEngine#cms recover identity default
Registering this node as Service Engine...
Sending identity recovery request with key default
Thu Jun 26 13:16:09 UTC 2003 [I] main: creating 24 messages
Thu Jun 26 13:16:09 UTC 2003 [I] main: creating 12 dispatchers
Thu Jun 26 13:16:09 UTC 2003 [I] main: Sending registration message to CDSM
10.107.192.168
There are no SE devices in CDN
register: Registration failed.
ServiceEngine#
```

Related Commands

cms enable

show cms

cms (global configuration)

To schedule maintenance and enable the Centralized Management System (CMS) on a given node, use the **cms** global configuration command. To negate these actions, use the **no** form of this command.

cms {**database maintenance** {**full** {**enable** | **schedule** *weekday* **at** *time*} | **regular** {**enable** | **schedule** *weekday* **at** *time*}} | **enable** | **rpc timeout** {**connection** *5-1800* | **incoming-wait** *10-600* | **transfer** *10-7200*}}

no cms {**database maintenance** {**full** {**enable** | **schedule** *weekday* **at** *time*} | **regular** {**enable** | **schedule** *weekday* **at** *time*}} | **enable** | **rpc timeout** {**connection** *5-1800* | **incoming-wait** *10-600* | **transfer** *10-7200*}}

Syntax Description

database maintenance	Configures the embedded database clean or reindex maintenance routine.
full	Configures the full maintenance routine and cleans the embedded database tables.
enable	Enables the full maintenance routine to be performed on the embedded database tables.
schedule	Sets the schedule for performing the maintenance routine.
weekday	Day of the week to start the maintenance routine. every-day Every day Fri every Friday Mon every Monday Sat every Saturday Sun every Sunday Thu every Thursday Tue every Tuesday Wed every Wednesday
at	Sets the maintenance schedule time of day to start the maintenance routine.
time	Time of day to start the maintenance routine (0–23:0–59) (hh:mm).
regular	Configures the regular maintenance routine and reindexes the embedded database tables.
enable	Enables the node CMS process.
rpc timeout	Configures the timeout values for remote procedure call connections.
connection	Specifies the maximum time to wait when making a connection.
5-1800	Timeout period in seconds. The default for the CDSM is 30 seconds; the default for the SE and the SR is 180 seconds.
incoming-wait	Specifies the maximum time to wait for a client response.
10-600	Timeout period in seconds. The default is 30 seconds.
transfer	Specifies the maximum time to allow a connection to remain open.
10-7200	Timeout period in seconds. The default is 300 seconds.

Defaults

database maintenance regular: enabled

database maintenance full: enabled

connection: 30 seconds for CDSM; 180 seconds for the SE and the SR

incoming wait: 30 seconds

transfer: 300 seconds

Command Modes

Global configuration

Usage Guidelines

Use the **cms database maintenance** command to schedule routine full maintenance cleaning (vacuuming) or a regular maintenance reindexing of the embedded database. The full maintenance routine runs only when the disk is more than 90 percent full and only runs once a week. Cleaning the tables returns reusable space to the database system.

The **cms enable** command automatically registers the node in the database management tables and enables the CMS process. The **no cms enable** command only stops the management services on the device and does not disable a primary sender. You can use the **cms deregister** command to remove a primary or backup sender SE from the CDS network and to disable communication between the two multicast senders.

Examples

The following example schedules a regular (reindexing) maintenance routine to start every Friday at 11:00 p.m.:

```
ServiceEngine(config)#cms database maintenance regular schedule Fri at 23:00
```

The following example shows how to enable the CMS process on an SE:

```
ServiceEngine(config)#cms enable
This operation needs to restart http proxy and streaming proxies/servers (if running) for
memory reconfiguration. Proceed? [no]yes
Registering this node as Service Engine...
Thu Jun 26 13:18:24 UTC 2003 [I] main: creating 24 messages
Thu Jun 26 13:18:25 UTC 2003 [I] main: creating 12 dispatchers
Thu Jun 26 13:18:25 UTC 2003 [I] main: Sending registration message to CDSM
10.107.192.168
Thu Jun 26 13:18:27 UTC 2003 [I] main: Connecting storeSetup for SE.
Thu Jun 26 13:18:27 UTC 2003 [I] main: Instantiating AStore
'com.cisco.unicorn.schema.PSqlStore'...
Thu Jun 26 13:18:28 UTC 2003 [I] main: Successfully connected to database
Thu Jun 26 13:18:28 UTC 2003 [I] main: Registering object factories for persistent
store...
Thu Jun 26 13:18:35 UTC 2003 [I] main: Dropped Sequence IDSET.
Thu Jun 26 13:18:35 UTC 2003 [I] main: Dropped Sequence GENSET.
Thu Jun 26 13:18:35 UTC 2003 [I] main: Dropped Table USER_TO_DOMAIN.
.
.
.
Thu Jun 26 13:18:39 UTC 2003 [I] main: Created Table FILE_CDSM.
Thu Jun 26 13:18:40 UTC 2003 [I] main: Created SYS_MESS_TIME_IDX index.
Thu Jun 26 13:18:40 UTC 2003 [I] main: Created SYS_MESS_NODE_IDX index.
Thu Jun 26 13:18:40 UTC 2003 [I] main: No Consistency check for store.
Thu Jun 26 13:18:40 UTC 2003 [I] main: Successfully created management tables
Thu Jun 26 13:18:40 UTC 2003 [I] main: Registering object factories for persistent
store...
```

```
Thu Jun 26 13:18:40 UTC 2003 [I] main: AStore Loading store data...
Thu Jun 26 13:18:41 UTC 2003 [I] main: ExtExpiresRecord Loaded 0 Expires records.
Thu Jun 26 13:18:41 UTC 2003 [I] main: Skipping Construction RdToClusterMappings on
non-CDSM node.
Thu Jun 26 13:18:41 UTC 2003 [I] main: AStore Done Loading. 336
Thu Jun 26 13:18:41 UTC 2003 [I] main: Created SYS_MESS_TIME_IDX index.
Thu Jun 26 13:18:41 UTC 2003 [I] main: Created SYS_MESS_NODE_IDX index.
Thu Jun 26 13:18:41 UTC 2003 [I] main: No Consistency check for store.
Thu Jun 26 13:18:41 UTC 2003 [I] main: Successfully initialized management tables
Node successfully registered with id 28940
Registration complete.
Warning: The device will now be managed by the CDSM. Any configuration changes
made via CLI on this device will be overwritten if they conflict with settings on the
CDSM.
Please preserve running configuration using 'copy running-config startup-config'.
Otherwise management service will not be started on reload and node will be shown
'offline' in CDSM UI.
management services enabled
ServiceEngine(config)#
```

Related Commands

cms database
cms deregister
show cms

configure

To enter global configuration mode, use the **configure** EXEC command. You must be in global configuration mode to enter global configuration commands.

configure

To exit global configuration mode, use the **end** or **exit** commands. In addition, you can press **Ctrl-Z** to exit from global configuration mode.

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Use this command to enter global configuration mode.

Examples

The following example shows how to enable global configuration mode:

```
ServiceEngine#configure
ServiceEngine(config)#
```

Related Commands

end
exit
show running-config
show startup-config

copy

To copy the configuration or image data from a source to a destination, use the **copy** EXEC command.

copy cdnfs disk *url sysfs-filename*

copy cdrom install *filedir filename*

copy disk {**ftp** {*hostname* | *ip-address*} *remotefiledir remotefilename localfilename* | **startup-config** *filename*}

copy ftp {**disk** {*hostname* | *ip-address*} *remotefiledir remotefilename localfilename* | **install** {*hostname* | *ip-address*} *remotefiledir remotefilename*}

copy http install {{*hostname* | *ip-address*} *remotefiledir remotefilename*} [**port** *port-num* [**proxy** {*hostname* | *ip-address*} | **username** *username password* [**proxy** {*hostname* | *ip-address*} *proxy_portnum*]] | **proxy** {*hostname* | *ip-address*} *proxy_portnum* | **username** *username password* [**proxy** {*hostname* | *ip-address*} *proxy_portnum*]]

copy running-config {**disk** *filename* | **startup-config** | *remotefilename*}

copy startup-config {**disk** *filename* | **running-config** | *remotefilename*}

copy system-status disk *filename*

copy tech-support {**disk** *filename* | *remotefilename*}

Syntax Description

cdnfs	Copies a file from the cdnfs to the sysfs.
disk	Copies a file to the disk.
url	URL of the cdnfs file to be copied to the sysfs.
sysfs-filename	Filename to be copied in the sysfs.
cdrom	Copies a file from the CD-ROM.
install	Installs the software release file.
filedir	Directory location of the software release file.
filename	Filename of the software release file.
disk	Copies a local disk file.
ftp	Copies to a file on an FTP server.
hostname	Hostname of the FTP server.
ip-address	IP address of the FTP server.
remotefiledir	Directory on the FTP server to which the local file is copied.
remotefilename	Name of the local file once it has been copied to the FTP server.
localfilename	Name of the local file to be copied.
startup-config	Copies the configuration file from the disk to startup configuration (NVRAM).
filename	Name of the existing configuration file.
ftp	Copies a file from an FTP server.
disk	Copies a file to a local disk.

hostname	Hostname of the FTP server.
ip-address	IP address of the FTP server.
remotefiledir	Directory on the FTP server where the file to be copied is located.
remotefilename	Name of the file to be copied to the local disk.
localfilename	Name of the copied file as it appears on the local disk.
install	Copies the file from an FTP server and installs the software release file to the local device.
hostname	Name of the FTP server.
ip-address	IP address of the FTP server.
remotefiledir	Remote file directory.
remotefilename	Remote filename.
http install	Copies the file from an HTTP server and installs the software release file on a local device.
hostname	Name of the HTTP server.
ip-address	IP address of the HTTP server.
remotefiledir	Remote file directory.
remotefilename	Remote filename.
port	(Optional) Specifies the port to connect to the HTTP server (default is 80).
port-num	HTTP server port number (1–65535).
proxy	Allows the request to be redirected to an HTTP proxy server.
hostname	Name of the HTTP server.
ip-address	IP address of the HTTP server.
proxy_portnum	HTTP proxy server port number (1–65535).
username	Specifies the username to access the HTTP proxy server.
username	User login name.
running-config	Copies the current system configuration.
disk	Copies the current system configuration to a disk file.
filename	Name of the file to be created on disk.
startup-config	Copies the running configuration to the startup configuration (NVRAM).
remotefilename	Remote filename of the configuration file to be created on the TFTP server. Use the complete pathname.
startup-config	Copies the startup configuration.
disk	Copies the startup configuration to a disk file.
filename	Name of the startup configuration file to be copied to the local disk.
running-config	Copies the startup configuration to a running configuration.
remotefilename	Remote filename of the startup configuration file to be created on the TFTP server. Use the complete pathname.
system-status disk	Copies the system status to a disk file.
filename	Name of the file to be created on the disk.
tech-support	Copies system information for technical support.
disk	Copies system information for technical support to a disk file.

filename	Name of the file to be created on disk.
remotefilename	Remote filename of the system information file to be created on the TFTP server. Use the complete pathname.

Defaults

HTTP server port: 80

Default working directory for sysfs files: /local1

Command Modes

EXEC

Usage Guidelines

The **copy cdnfs** EXEC command copies data files out of the cdnfs to the sysfs for further processing. For example, you can use the **install** *imagefilename* EXEC command to provide the copied files to the command.

The **copy disk ftp** command copies files from a sysfs partition to an FTP server. The **copy disk startup-config** command copies a startup configuration file to NVRAM.

The **copy ftp disk** command copies a file from an FTP server to a sysfs partition.

Use the **copy ftp install** command to install an image file from an FTP server. Part of the image goes to the disk and part goes to the flash memory.

Use the **copy http install** command to install an image file from an HTTP server and install it on a local device. It transfers the image from an HTTP server to the SE using HTTP as the transport protocol and installs the software on the device. Part of the image goes to the disk and part goes to the flash memory. You can also use this command to redirect your transfer to a different location or HTTP proxy server, by specifying the **proxy** *hostname* | *ip-address* option. A username and a password will have to be authenticated with the remote HTTP server if the server is password protected and requires authentication before the transfer of the software release file to the SE is allowed.

Use the **copy cdrom install** option to install the image from the rescue CD.

```
ServiceEngine#copy cdrom install /images CDS24.bin
```

Use the **copy running-config** command to copy the running system configuration to a sysfs partition or flash memory. The **copy running-config startup-config** command is equivalent to the **write memory** command.

The **copy startup-config** command copies the startup configuration file to a sysfs partition.

The **copy system-status** command creates a file on a sysfs partition containing hardware and software status information.

The **copy tech-support tftp** command can copy technical support information to a a sysfs partition.

Related Commands

install
reload
show running-config
show startup-config
write

cpfile

To make a copy of a file, use the **cpfile** EXEC command.

cpfile *oldfilename newfilename*

Syntax Description

oldfilename	Name of the file to copy.
newfilename	Name of the copy to be created.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Use this command to create a copy of a file. Only sysfs files can be copied.

Examples

The following example shows how to create a copy of a file:

```
ServiceEngine#cpfile syslog.txt syslog.txt.save
```

Related Commands

copy
dir
lls
ls
mkfile
rename
rmdir

debug

To monitor and record caching application functions, use the **debug** EXEC command. To disable **debug**, use the **no** form of this command.

debug *option*

no debug *option*

Syntax Description

option	Specifies the debugger type; see the "Usage Guidelines" section for valid values.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Note We recommend that you use the **debug** command only at the direction of Cisco TAC because the SE performance is affected when you enter the **debug** command.

You can use the **logging disk priority debug** global configuration command with the **debug** command. This configuration causes the debugging messages to be logged in the syslog file, which is available in the /local1 directory by default. You can then download the messages from the SE, copy them to a local disk file (for example, using the **copy disk ftp** command), and forward the logs to Cisco TAC for further investigation. By default, system log messages are logged to the console and you need to copy and paste the output to a file. However, this method of obtaining logs is more prone to errors than capturing all messages in the syslog.txt file. When you use system logging to a disk file instead of system logging to a console, there is no immediate feedback that debug logging is occurring, except that the syslog.txt file gets larger (you can track the lines added to the syslog.txt file by entering the **type-tail syslog.txt follow** command). When you have completed downloading the system logs to a local disk, you must disable the debugging functions by using the **undebug** command (see the "undebug" section on page -447 for more details), and reset the level of logging disk priority to any other setting that you want (for example, **notice** priority).

Valid values for *option* are as follows:

access-lists 300	Debugs the access control list.
dump	Dumps the access control list contents.
query	Queries the access control list configuration.
username *username*	Queries the access control list username.
groupname *groupnames*	Queries the access control list group name or names of groups of which the user is a member. Each group name must be separated by a comma.

acquirer	Debugs the acquirer.
error	Sets the debug level to error.
trace	Sets the debug level to trace.
all	Enables all debugging.
authentication	Debugs authentication.
user	Debugs the user login against the system authentication.
authsvr	Debugs the Autnentication Server.
error	Sets the debug level to error.
trace	Sets the debug level to trace.
bandwidth	Debugs the bandwidth module.
advanced	Advanced bandwidth controller debug commands.
error	Sets the debug level to error.
trace	Sets the debug level to trace.
buf	Debugs the buffer manager.
all	Debugs all buffer manager functions.
dmbuf	Debugs the buffer manager dmbuf.
dmsg	Debugs the buffer manager dmsg.
cache-content	Debugs the caching service.
all	(Optional) Sets the debug level to all.
error	(Optional) Sets the debug level to error.
trace	(Optional) Sets the debug level to trace.
cache-router	Debugs the caching router.
error	Sets the debug level to error.
trace	Sets the debug level to trace.
cdnfs	Debugs the CDS network file system (cdnfs).
cli	Debugs the CLI command.
all	Debugs all CLI commands.
bin	Debugs the CLI command binary program.
parser	Debugs the CLI command parser.
cms	Debugs the CMS.
dataserver	Debugs the data server.
all	Debuts all data server functions.
clientlib	Debugs the data server client library module.
server	Debugs the data server module.

dfs	Debugs the DFS.
all	Sets the debug level to all.
api	Debugs the DFS application API.
diskcache	Debugs the DFS in-memory disk-directory cache management.
memcache	Debugs the DFS in-memory cache.
rawio	Debugs the DFS raw disk I/O.
dhcp	Debugs the DHCP.
distribution	Debugs the distribution components.
all	Debugs all distribution components.
error	Debugs all distribution components to error level 1 (show error).
trace	Debugs all distribution components to trace level 2 (show error and trace).
metadata-receiver	Debugs the metadata receiver distribution component.
error	Debugs the metadata receiver distribution component to error level 1.
trace	Debugs the metadata receiver distribution component to trace level 2.
metadata-sender	Debugs the metadata sender distribution component.
error	Debugs the metadata sender distribution component to error level 1.
trace	Debugs the metadata sender distribution component to trace level 2.
mcast-receiver	Debugs the multicast receiver distribution component.
error	Debugs the multicast receiver distribution component to error level 1.
trace	Debugs the multicast receiver distribution component to trace level 2.
mcast-sender	Debugs the multicast sender distribution component.
error	Debugs the multicast sender distribution component to error level 1.
trace	Debugs the multicast sender distribution component to trace level 2.
unicast-data-receiver	Debugs the unicast receiver distribution component.
error	Debugs the unicast receiver distribution component to error level 1.
trace	Debugs the unicast receiver distribution component to trace level 2.
unicast-data-sender	Debugs the unicast sender distribution component.
error	Debugs the unicast sender distribution component to error level 1.
trace	Debugs the unicast sender distribution component to trace level 2.

emdb	Debugs the embedded database.
level	(Optional) Debug level.
(0-16)	Debug level 0 through 16.
flash-media-streaming	Debugs Flash Media Streaming.
error	Debugs the Flash Media Streaming log level error.
trace	Debugs the Flash Media Streaming log level debug.
icap	Debugs ICAP.
all	Debugs both ICAP client and ICAP daemon processing.
client	Debugs the ICAP client (caching proxy) processing.
daemon	Debugs the ICAP daemon processing.
logging	Debugs logging.
all	Debugs all logging functions.
malloc	Debug commands for memory allocation.
cache-app	Debugging commands for cache application memory allocation.
all	Sets the debug level to all.
caller-accounting	Collects statistics for every distinct allocation call-stack.
catch-double-free	Alerts if application attempts to release the same memory twice.
check-boundaries	Checks boundary over and under run scribble.
check-free-chunks	Checks if free chunks are over-written after release.
clear-on-alloc	Ensures all allocations are zero-cleared.
statistics	Allocator use statistical summary.
dns-server	DNS Caching Service memory allocation debugging.
all	Sets the debug level to all.
caller-accounting	Collects statistics for every distinct allocation call-stack.
catch-double-free	Alerts if application attempts to release the same memory twice.
check-boundaries	Checks boundary over and under run scribble.
icap	ICAP Service memory allocation debugging.
caller-accounting	Collects statistics for every distinct allocation call-stack.
catch-double-free	Alerts if application attempts to release the same memory twice.
check-boundaries	Checks boundary over and under run scribble.
log-directory	Memory allocation debugging log directory.
word	Directory path name.
movie-streamer	Debug commands for the Movie Streamer.
error	Sets the debug level to error.
trace	Sets the debug level to trace.
ntp	Debugs NTP.

qos	Debug commands for the QoS component.
policy service	Debug commands for the policy service.
error	Sets the debug level to error.
trace	Sets the debug level to trace.
rbcp	Debugs the RBCP (Router Blade Configuration Protocol) functions.
rpc	Displays the remote procedure calls (RPC) logs.
detail	Displays the RPC logs of priority “detail” level or higher.
trace	Displays the RPC logs of priority “trace” level or higher.
rtsp	Debugs the RTSP functions.
gateway	Debugs the RTSP gateway.
error	Debugs the RTSP gateway to level 1 (show error).
trace	Debugs the RTSP gateway to level 2 (show error and trace).
rule	Debugs the Rules Template.
action	Debugs the rule action.
all	Debugs all rule functions.
pattern	Debugs the rule pattern.
service-router	Debug commands for the service router.
servicemonitor	Debug commands for the service monitor.
session-manager	Session manager debug commands.
critical	Sets the debug level to critical.
error	Sets the debug level to error.
trace	Sets the debug level to trace.
snmp	Debugs SNMP.
all	Debugs all SNMP functions.
cli	Debugs the SNMP CLI.
main	Debugs the SNMP main.
mib	Debugs the SNMP MIB.
traps	Debugs the SNMP traps.
standby	Debugs standby.
all	(Optional) Debugs all standby functions.
stats	Debugs the statistics.
all	Debugs all statistics functions.
collection	Debugs the statistics collection.
computation	Debugs the statistics computation.
history	Debugs the statistics history.

translog	Debugs the transaction logging.
all	Debugs all transaction logging.
archive	Debugs the transaction log archive.
export	Debugs the transaction log FTP export.
uns	Unified naming service debug commands.
all	(Optional) Sets the debug level to all.
error	(Optional) Sets the debug level to error.
trace	(Optional) Sets the debug level to trace.
webengine	WebEngine debug commands.
error	Sets the debug level to error.
trace	Sets the debug level to trace.
wi	Debugs the web interface.
wmt	Debugs the WMT component.
error	Debugs the WMT level 1 functionality. For more information, see the "Using WMT Error Logging" section on page 2-78.
client-ip *cl-ip-address*	(Optional) Debugs the request from a specific client IP address to level 1 (show error).
server-ip *sv-ip-address*	(Optional) Debugs the request to a specific server IP address to level 1 (show error).
trace	Debugs the WMT level 2 functionality.
client-ip *cl-ip-address*	(Optional) Debugs the request from a specific client IP address to level 2 (show error and trace).
server-ip *sv-ip-address*	(Optional) Debugs the request to a specific server IP address to level 2 (show error and trace).

Debugging Cdnfs

You can use the **debug cdnfs** command to monitor the lookup and serving of pre-positioned files. If pre-positioned files are available in cdnfs but are not served properly, you can use cdnfs debug.

Using WMT Error Logging

In the Internet Streamer CDS Release 2.4 software, WMT error logging was enhanced. More information is now logged about the following events:

- When a WMT client is abruptly disconnected
- When any WMT streams are cleared on the SE

Error logs are in the same format and location as syslogs. The WMT log messages are logged to /local1/errorlog/wmt_errorlog.current.

You can configure the SE for WMT error logging by using the **debug wmt error** EXEC command. This command debugs WMT level 1 functionality.

Logging WMT Client Disconnects

When a WMT client is disconnected abruptly, the reasons for the client disconnect (for example, the request was blocked by the rules, the maximum incoming or outgoing bit-rate limit was reached, the maximum incoming or outgoing bandwidth limit was reached) are logged in Internet Streamer CDS software error logs.

The client information includes the client IP address, the server IP address, the requested URL, the client protocol, the version of the client media player, the number of packets that the client received, and the number of packets that the server sent.

Related Commands

logging
show debugging
undebug

delfile

To delete a file, use the **delfile** EXEC command.

delfile *filename*

Syntax Description

filename	Name of the file to delete.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Use this command to remove a file from a sysfs partition.

Examples

The following example shows how to delete a file:

```
ServiceEngine#delfile /local1/tempfile
```

Related Commands

cpfile
deltree
mkdir
mkfile
rmdir

deltree

To remove a directory with its subdirectories and files, use the **deltree** EXEC command.

deltree *directory*

Syntax Description

directory	Name of the directory tree to delete.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Use this command to remove a directory and all files within the directory from the SE sysfs file system. Do not remove files or directories required for proper SE functioning.

Examples

The following example shows how to delete a directory from the /local1 directory:

```
ServiceEngine#deltree /local1/testdir
```

Related Commands

delfile
mkdir
mkfile
rmdir

device

To configure the mode of operation on a device as a CDSM, SE or SR, use the **device** global configuration command. To reset the mode of operation on a device, use the **no** form of this command.

device mode {**content-delivery-system-manager** | **service-engine** | **service-router**}

no device mode {**content-delivery-system-manager** | **service-engine** | **service-router**}

Syntax Description

mode	Sets the mode of operation of a device to CDSM, SE or SR.
content-delivery-system-manager	Configures the device operation mode as a CDSM.
service-engine	Configures the device operation mode as an SE.
service-router	Configures the device operation mode as an SR.

Defaults

The default device operation mode is SE.

Command Modes

Global configuration

Usage Guidelines

A CDSM is the content management and device management station of an CDS network that allows you to specify what content is to be distributed, and where the content should be distributed. If an SR is deployed in the CDS network, the SR redirects the client based on redirecting policy. An SE is the device that serves content to the clients. There are typically many SEs deployed in an CDS network, each serving a local set of clients. IP/TV brings movie-quality video over enterprise networks to the desktop of the CDS network user.

Because different device modes require disk space to be used in different ways, disk space must also be configured when the device mode changes from being an SE or SR to CDSM (or the other way around). You must reboot the device before the configuration changes to the device mode take effect.

Disks must be configured before device configuration is changed. Use the **disk configure** command to configure the disk before reconfiguring the device to the SE or SR mode. Disk configuration changes using the **disk configure** command takes effect after the next device reboot.

To enable CDS network-related applications and services, use the **cms enable** command. Use the **no** form of this command to disable the CDS network.

All CDS devices ship from the factory as SEs. Before configuring network settings for CDSMs and SRs using the CLI, you must change the device from an SE to the proper device mode.

Configuring the device mode is not a supported option on all hardware models. However, you can configure some hardware models to operate as any one of the four content networking device types. Devices that can be reconfigured using the **device mode** global configuration command are shipped from the factory by default as SEs.

To change the device mode of your SE, you must also configure the disk space allocations, as required by the different device modes, and reboot the device for the new configuration to take effect.

When you change the device mode of an SE to an SR or CDSM, you may need to reconfigure the system file system (sysfs). However, SRs and CDSMs do not require any disk space other than sysfs. When you change the device mode to an SR or a CDSM, disk configuration changes are not required because the device already has some space allotted for sysfs. sysfs disk space is always preconfigured on a factory-fresh CDS network device. See the "Disk Space-Allocation Guidelines for Service Routers" section on page 2-88 and "Disk Space-Allocation Guidelines for CDSMs" section on page 2-88 for more information.

If you are changing the device mode of an SR or a CDSM back to an SE, you must configure disk space allocations for the caching, pre-positioning (cdnfs) and system use (sysfs) file systems that are used on the SE. You can configure disk space allocations either before or after you change the device mode to an SE.

Examples

The following examples show the configuration from the default mode, SE, to the CDSM, SR, and SE modes:

```
ServiceEngine(config)#device mode content-delivery-system-manager
```

```
CDSM(config)#device mode service-router
```

```
ServiceRouter(config)#device mode service-engine
```

Related Commands

show device-mode

dir

To view a long list of files in a directory, use the **dir** EXEC command.

dir [*directory*]

Syntax Description

directory	(Optional) Name of the directory to list.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Use this command to view a detailed list of files contained within the working directory, including names, sizes, and time created. The equivalent command is **lls**.

Examples

The following example shows how to view a list of files in a directory:

```
ServiceEngine#dir
size            time of last change                name
--------------  -------------------------          -----------
       3931934  Tue Sep 19 10:41:32 2000           errlog-cache-20000918-164015
           431  Mon Sep 18 16:57:40 2000           ii.cfg
           431  Mon Sep 18 17:27:46 2000           ii4.cfg
           431  Mon Sep 18 16:54:50 2000           iii.cfg
          1453  Tue Sep 19 10:34:03 2000           syslog.txt
          1024  Tue Sep 19 10:41:31 2000  <DIR>    testdir
```

Related Commands

lls
ls

direct-server-return

To enable a VIP for direct server return, use the **direct-server-return** global configuration command. To disable direct server return, use the **no** form of this command.

direct-server-return vip *ip address*

no direct-server-return vip *ip address*

Syntax Description

vip	Specifies the VIP for direct-server-return.
ip address	VIP for direct-server-return.

Defaults

No default behavior or values.

Command Modes

Global configuration

Usage Guidelines

Direct Server Return (DSR) is a method used by load balancer servers in a load balancing configuration. DSR responds directly to the client, bypassing the load balancer in the response path. Table 2-5 shows the Direct Server Return flow.

Table 2-5 Direct Server Return Flow

Step	Process	Source IP	Destination IP	Destination MAC
Step 1	Client to load balancer	171.71.50.140	170.1.1.45	00:30:48:C3:C7:C5
Step 2	Load balancer to SR	171.71.50.140	170.1.1.45	00:14:5E:83:6E:7E
Step 3	SR to client	170.1.1.45	171.71.50.140	Default Gateway MAC

Examples

The following example shows how to enable direct server return:

```
ServiceEngine(config)#direct-server-return vip 1.1.1.1
ServiceEngine(config)#
```

Related Commands

show direct-server-return

disable

To turn off privileged EXEC commands, use the **disable** EXEC command.

disable

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

The **disable** command places you in the user-level EXEC shell. To turn privileged EXEC mode back on, use the **enable** command.

Examples

The following example shows how to enter the user-level EXEC mode:

```
ServiceEngine#disable
ServiceEngine>
```

Related Commands

enable

disk (EXEC)

To configure disks and allocate disk space for devices that are using the CDS software, use the **disk** EXEC command.

disk mark *diskname* {**bad** | **good**}

disk recover-system-volumes

disk reformat *diskname*

disk unuse *diskname*

Syntax Description

mark	Marks a disk drive as good or bad.
diskname	Name of the disk to be marked (disk01, disk02, and so on).
bad	Marks the disk drive as bad.
good	Marks the disk drive as good.
recover--system-volumes	Erases all SYSTEM and SYSFS volumes.
reformat	Performs a low-level format of the SCSI, IDE, or SATA disks and remaps disk errors.
diskname	Name of the disk to be reformatted (disk01, disk02, and so on).
unuse	Stops applications from using a disk drive.
diskname	Name of the disk to be stopped for application use (disk01, disk02, and so on).

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

The disk space in the CDS software is allocated on a per-file system basis, rather than on a per-disk basis. You can configure your overall disk storage allocations according to the kinds of client protocols that you expect to use and the amount of storage that you need to provide for each of the functions.

Note For details on the Cisco Internet Streamer CDS software disk storage and configuration requirements for SEs, see the *Cisco Internet Streamer CDS 2.4 Software Configuration Guide*.

The cndfs and sysfs partitions use the ext2 file system. With ext2 file systems, if the system crashed or if the system is not shut down cleanly, a file system check of these partitions takes a long time. If there are sector failures on the disk, the time to perform a file system check with an ext2 file system increases even more. By migrating to the ext3 file system, the amount of time required to perform a file system check of the cndfs and sysfs partitions is decreased, which increases the availability of the SE. If you are upgrading from an earlier release of the CDS software, the ext2 file system is automatically converted to the ext3 file system.

The cdnfs amounts are reported by the actual usable amounts of storage for applications. Due to the internal file system overhead of approximately 3 percent, the reported amounts may be smaller than what you configured.

To view disk details, use the **show disks details**.

Note The **show disks details** command shows the amount of disk space that is allocated to system use. This detail is not shown by using the **show disks current** command.

To show the space allocation in each individual file system type, use the **show statistics cdnfs** command.

Note For information on disk allocation guidelines for SEs, see the *Cisco Internet Streamer CDS 2.4 Software Configuration Guide*.

For higher-end models that might be used as a dedicated HTTP cache or RealProxy cache, you could give cache storage more disk space.

After upgrading from an earlier release of Internet Streamer CDS software to Cisco Internet Streamer Release 2.4 software and later releases, your disk space allocation remains the same as previously configured.

Disk Space-Allocation Guidelines for Service Routers

In Cisco Internet Streamer Release 2.4 software, SRs are used as DNS servers for the delegated DNS zone used in simplified hybrid routing. The DNS servers do not store any content and do not participate in acquisition or distribution of the pre-positioned content. The only disk space that needs to be configured on the SR is the sysfs.

Disk Space-Allocation Guidelines for CDSMs

CDSMs are used to manage content distribution for CDS networks. Because the CDSM does not store the content, the only file system that needs to be configured is the sysfs.

Remapping of Bad Sectors on Disk Drives

The **disk reformat** *diskname* EXEC command performs a low-level format of the SCSI, IDE, or SATA disks. This command erases all of the content on the disk.

If a disk drive continues to report a failure after you have used the **disk reformat** command, you must replace the disk drive.

Caution Be careful when using the **disk reformat** *diskname* command because this command causes all content on the specified disk to be deleted.

In Cisco Internet Streamer Release 2.4 software, SCSI and Serial Advanced Technology Attachment (SATA) drives can be reformatted.

Stopping Applications from Using a Disk Drive

The **disk unuse** EXEC command allows you to stop applications from using a specific disk drive (for example, disk01) without having to reboot the device:

```
ServiceEngine# disk unuse disk01
```

The **disk unuse** command has the following behavior:

1. Cannot be used with SYSFS disk if the state of RAID-1 is not “Normal”.
2. Cannot be used with the cdnfs disk, which contains the “/uns-symlink-tree” directory.
3. Can be used with any disk except as in scenario 1 and 2 above.

Examples

The following examples show usage of the **disk unuse** command and the resultant actions:

```
ServiceEngine#disk unuse disk00
disk00 has key CDNFS data and can not be unused!

ServiceEngine#disk unuse disk01
This will restart applications currently using disk01
and unmount all partitions on disk01.
Do you want to continue? (Yes/No): yes
[WARNING] CDNFS and RAID SYSTEM partitions detected on disk01
[WARNING] Unusing a RAID SYSTEM disk results in boot-time RAID conflicts that cause the
drive to be erased and repartitioned. This has little effect on RAID volumes,
as their data will resync. However, any CDNFS data on the drive will be lost!
Unuse disk01, erasing all CDNFS data? (Yes/No): yes
disk01 is now unused

ServiceEngine#disk unuse disk02
This will restart applications currently using disk02
and unmount all partitions on disk02.
Do you want to continue? (Yes/No): yes
disk02 is now unused
```

The following example shows how to display the current disk space configuration:

```
ServiceEngine#show disks current
Local disks:
    SYSFS 32.0GB 0.7%
    CDNFS 4616.0GB 99.3%
```

The following example shows how to view disk details:

```
ServiceEngine#show disks details
disk00: Normal          (h02 c00 i00 100 -       mptsas)  476937MB(465.8GB)
        disk00/04: SYSFS         32765MB( 32.0GB) mounted at /local1
        disk00/05: CDNFS        434445MB(424.3GB) mounted internally
        System use:               9726MB(  9.5GB)
        FREE:                        0MB(  0.0GB)
disk01: Normal          (h02 c00 i01 100 -       mptsas)  476937MB(465.8GB)
        disk01/04: SYSFS         32765MB( 32.0GB) mounted at /local1
        disk01/05: CDNFS        434445MB(424.3GB) mounted internally
        System use:               9726MB(  9.5GB)
        FREE:                        0MB(  0.0GB)
disk02: Normal          (h02 c00 i02 100 -       mptsas)  476937MB(465.8GB)
        disk02/01: CDNFS        476929MB(465.8GB) mounted internally
        System use:                  7MB(  0.0GB)
        FREE:                        0MB(  0.0GB)
```

The following examples show how to view space allocation in each file system type:

```
ServiceEngine#show statistics cdnfs

CDNFS Statistics:
------------------
Volume on :
  size of physical filesystem:            444740904 KB
  space assigned for CDNFS purposes:      444740904 KB
  number of CDNFS entries:                       40 entries
  space reserved for CDNFS entries:        436011947 KB
  available space for new entries:          8728957 KB
  physical filesystem space in use:        435593864 KB
  physical filesystem space free:           9147040 KB
  physical filesystem percentage in use:         98 %

Volume on :
  size of physical filesystem:             444740904 KB
  space assigned for CDNFS purposes:       444740904 KB
  number of CDNFS entries:                        43 entries
  space reserved for CDNFS entries:        436011384 KB
  available space for new entries:          8729520 KB
  physical filesystem space in use:        435593720 KB
  physical filesystem space free:           9147184 KB
  physical filesystem percentage in use:         98 %

Volume on :
  size of physical filesystem:             488244924 KB
  space assigned for CDNFS purposes:       488244924 KB
  number of CDNFS entries:                        48 entries
  space reserved for CDNFS entries:        479612533 KB
  available space for new entries:          8632391 KB
  physical filesystem space in use:        479152708 KB
  physical filesystem space free:           9092216 KB
  physical filesystem percentage in use:         99 %
```

Related Commands

disk (global configuration mode)
show cdnfs
show disks
show disks details
show statistics

disk (global configuration)

To configure how disk errors should be handled and to define a disk device error-handling threshold, use the **disk** global configuration command. To remove the device error-handling options, use the **no** form of this command.

disk error-handling {**reload** | **threshold** *number*}

no disk error-handling {**reload** | **threshold** *number*}

Syntax Description

error-handling	Configures disk error handling.
reload	Reloads the disk if the system file system (sysfs) (disk00) has problems.
threshold	Sets the number of disk errors allowed before the disk is marked as bad.
number	Number of disk errors allowed before the disk is marked as bad (0–100). The default is 1. The value 0 means that the disk should never be marked as bad.

Defaults

error-handling threshold *number*: 10

Command Modes

Global configuration

Usage Guidelines

In order to operate properly, the SE must have critical disk drives. A critical disk drive is the first disk drive that also contains the first sysfs (system file system) partition. It is referred to as disk00.

The sysfs partition is used to store log files, including transaction logs, system logs (syslogs), and internal debugging logs. It can also be used to store image files and configuration files on an SE.

Note A critical drive is a disk drive that is either disk00 or a disk drive that contains the first sysfs partition. Smaller single disk drive SEs have only one critical disk drive. Higher-end SEs that have more than one disk drive may have more than one critical disk drive.

When an SE is booted and a critical disk drive is not detected at system startup time, the CDS system on the SE runs at a degraded state. If one of the critical disk drives goes bad at run time, the CDS system applications can malfunction, hang, or crash, or the CDS system can hang or crash. You must monitor the critical disk drives on an SE and report any disk drive errors to Cisco TAC.

With an CDS system, a disk device error is defined as any of the following events:

- A Small Computer Systems Interface (SCSI) or Integrated Drive Electronics (IDE) device error is printed by a Linux kernel.
- A disk device access by an application (for example, an open(2), read(2), or write(2) system call) fails with an EIO error code.
- A disk device that existed at startup time is not accessible at run time.

The disk status is recorded in flash (nonvolatile storage). When an error on an SE disk device occurs, a message is written to the system log (syslog) if the sysfs partition is still intact, and an SNMP trap is generated if SNMP is configured on the SE.

In addition to tracking the state of critical disk drives, you can define a disk device error-handling threshold on the SE. If the number of disk device errors reaches the specified threshold, the corresponding disk device is automatically marked as bad. The CDS system does not stop using the bad disk device immediately; it stops using the bad disk drive after the next reboot.

If the specified threshold is exceeded, the SE either records this event or reboots. If the automatic reload feature is enabled and this threshold is exceeded, then the CDS system automatically reboots the SE. For more information about specifying this threshold, see the "Specifying the Disk Error-Handling Threshold" section on page 2-92.

In Cisco Internet Streamer Release 2.4 software, you can remap bad (but unused) sectors on a SCSI drive and SATA drives.

Specifying the Disk Error-Handling Threshold

In Cisco Internet Streamer CDS Release 2.4 software, you can configure a disk error-handling threshold. This threshold determines how many disk errors can be detected before the disk drive is automatically marked as bad. By default, this threshold is set to 10.

The **disk error-handling threshold** option determines how many disk errors can be detected before the disk drive is automatically marked as bad. By default, this threshold is set to 10.

To change the default threshold, use the **disk error-handling threshold** global configuration command. Specify 0 if you never want the disk drive to be marked as bad.

If the bad disk drive is a critical disk drive, and the automatic reload feature (**disk error-handling reload** command) is enabled, then the Internet Streamer CDS software marks the disk drive as bad and the SE is automatically reloaded. After the SE is reloaded, a syslog message and an SNMP trap are generated.

By default, the automatic reload feature is disabled on an SE. To enable the automatic reload feature, use the **disk error-handling reload** global configuration command. After enabling the automatic reload feature, use the **no disk error-handling reload** global configuration command to disable it.

Examples

The following example shows that five disk drive errors for a particular disk drive (for example, disk00) will be allowed before the disk drive is automatically marked as bad:

```
ServiceEngine(config)# disk error-handling threshold 5
```

Related Commands

disk (EXEC mode)
show disks
show disks details

distribution

To reschedule and refresh content redistribution for a specified delivery service ID or name, use the **distribution** EXEC command.

distribution {**failover** {**delivery-service-id** *delivery-service-num* | **delivery-service-name** *name*} [**force**] | **fallback** {**delivery-service-id** *delivery-service-num* | **delivery-service-name** *name*}}

distribution primary-ip-fallback {**forwarder-id** *forwarder-num* | **forwarder-name** *name*}

distribution refresh {**meta-data delivery-service-id** *delivery-service-num* | **object** *object-url*}

Syntax Description

failover	Triggers the root or forwarder SE to fail over and make this SE the temporary root SE.
delivery-service-id	Specifies the delivery service ID to be used.
delivery-service-num	Delivery service number (0–4294967295).
delivery-service-name	Specifies the delivery service name descriptor to be used.
name	Delivery service name.
force	(Optional) Forces a failover regardless of whether the root or forwarder SE is active.
fallback	Forces the temporary root SE to become a receiver SE.
primary-ip-fallback	Triggers the downstream receiver SEs to contact a forwarder using the forwarder's primary IP address. For more information, see the "distribution primary-ip-fallback Command" section on page 2-94.
forwarder-id	Specifies the forwarder SE ID that is contacted by the receiver SE.
forwarder-num	Forwarder SE ID.
forwarder-name	Specifies the name of the forwarder SE that is contacted by the receiver SE.
name	Forwarder SE name.
refresh	Forces the redistribution of content to be refreshed on every SE.
meta-data	Forces the redistribution of metadata to be refreshed on every SE.
delivery-service-id	Specifies the delivery service ID to be used in the distribution.
delivery-service-num	Delivery service number (0–4294967295).
object	Forces the distribution of objects to be refreshed on every SE.
object-url	Specifies the object URL that needs to be refreshed on every SE.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

When the root SE fails, use the **distribution failover** EXEC command on an SE that is going to be the temporary root SE to trigger an immediate failover to the temporary root SE if you do not want to wait for the automatic failover process to occur. When you enter this command, the current SE becomes the temporary root SE if its forwarder is an inactive root SE. If the root SE has not failed, a failover to the temporary root SE does not occur if you use the **distribution failover** EXEC command. Use the **distribution failover force** command to force a failover even if the root SE is active.

Use the **distribution fallback** command on an SE that is currently the temporary root SE to cause it to become a receiver SE.

Use the **distribution refresh meta-data** {**delivery-service-id** *delivery-service-num*} command to request that the metadata receiver repeat a previous request for all the content metadata for the specified delivery service from its forwarder SE. This method allows you to start over if the metadata receiver fails to replicate some metadata properly. The content metadata (machine-readable information that describes the characteristics of the content) must be distributed to a receiver first before the content can be replicated. The content metadata helps to define what content to retrieve, how content is retrieved, how recently the content has been updated, how the content is to be pre-positioned (for example, expiration time), and so forth. The metadata is always distributed using unicast. The content, however, can be replicated using unicast.

Use the **distribution refresh object** *object-url* command to reissue a request for unicast distribution of the specified object. This command lets you obtain a new copy of an object if there is a corrupted copy on the SE. After you enter this command, if the distribution is unicast, the unicast receiver reissues the request to its forwarder SE. The old content on the SE is removed and a new copy is replicated.

NACK Interval Multiplier

To identify missing content and trigger a resend of a file, receiver SEs send a negative acknowledgement (NACK) message to the sender SE. NACK messages generated by many receiver SEs could generate more traffic than the sender can handle. Cisco Internet Streamer Release 2.4 software allows you to adjust the average interval between NACKs by configuring a NACK interval multiplier for an individual receiver SE. This value (an integer between 0.1–10) adjusts the default average NACK interval (the default is 20 minutes) by the value configured as the interval multiplier. For example, if you set the NACK interval multiplier to 3, the interval between NACKs becomes 20 minutes x 3, or 60 minutes. This adjustment can be made as needed by choosing **Devices > Devices > Prepositioning > Distribution** in the CDSM GUI.

distribution primary-ip-fallback Command

When downstream receiver SEs at the edge of the network try to access a forwarder SE that is inside a NAT firewall, those receiver SEs that are inside the same NAT use one IP address (called the inside local IP address) to access the forwarder, but other receiver SEs that are outside the NAT need to use a different forwarder’s IP address (called the inside global IP address or NAT address) to access the forwarder. A forwarder SE registers the IP address configured on its primary interface with the CDSM, and the CDSM uses the primary IP address for communication with devices in the CDS network. If the registered primary IP address is the inside local IP address and the forwarder is behind a NAT firewall, a receiver that is not inside the same NAT as the forwarder cannot contact it without special configuration. All other receivers inside the NAT use the inside local IP address to contact the forwarder that resides inside the NAT.

Cisco Internet Streamer Release 2.4 software supports NAT for unicast distribution (see the “NAT Firewall” section on page 2-95 for more information). When the receiver SE polls its forwarder from an upstream location for the content metadata or content, the receiver first connects to the forwarder using the forwarder’s primary IP address. If it fails and the forwarder’s NAT address has been configured, then the unicast receiver tries to poll the forwarder using the forwarder’s NAT address. If the receiver polls the forwarder successfully using the NAT address, the receiver continues to use the forwarder’s NAT address during the subsequent polling intervals with the same forwarder. The unicast receiver retries to connect to the forwarder using the forwarder’s primary IP address only after one hour. Even if the unicast receiver is able to poll the forwarder using the forwarder’s primary IP address, it would take one hour for the receiver to fall back to the forwarder's primary IP address automatically. You can use the

distribution primary-ip-fallback command to enable the receiver that is using the NAT address of the forwarder to fall back to the primary IP address immediately, if you are certain that the forwarder's primary IP address is working.

NAT Firewall

Network Address Translation (NAT) enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT is configured on the firewall at the border of a stub domain (referred to as the inside network) and a public network such as the Internet (referred to as the outside network). NAT translates the internal local addresses to globally unique IP addresses before sending packets to the outside network. You can configure NAT to advertise only one address for the entire network to the outside world. This configuration provides additional security, effectively hiding the entire internal network from the world behind that address. NAT has the dual functionality of security and address conservation and is typically implemented in remote access environments.

In the inside network's domain, hosts have addresses in the one address space. While on the outside, they appear to have addresses in another address space when NAT is configured. The first address space is referred to as the local address space while the second is referred to as the global address space.

Hosts in outside networks can be subject to translation and can have local and global addresses.

NAT uses the following definitions:

- Inside local address—The IP address that is assigned to a host on the inside network. The address is probably not a legitimate IP address assigned by the Network Information Center (NIC) or service provider.
- Inside global address—A legitimate IP address (assigned by the NIC or service provider) that represents one or more inside local IP addresses to the outside world.
- Outside local address—The IP address of an outside host as it appears to the inside network. Not necessarily a legitimate address, it was allocated from an address space routable on the inside.
- Outside global address—The IP address assigned to a host on the outside network by the host's owner. The address was allocated from a globally routable address or network space.

Related Commands

show statistics distribution

dnslookup

To resolve a host or domain name to an IP address, use the **dnslookup** EXEC command.

dnslookup {*hostname* | *domainname*}

Syntax Description

hostname	Name of host on the network.
domainname	Name of domain.

Defaults

No default behavior or values.

Command Modes

EXEC

Examples

The following examples show that the **dnslookup** command is used to resolve the hostname *myhost* to IP address 172.31.69.11, *cisco.com* to IP address 192.168.219.25, and an IP address used as a hostname to 10.0.11.0:

```
ServiceEngine#dnslookup myhost
official hostname: myhost.cisco.com
          address: 172.31.69.11

ServiceEngine#dnslookup cisco.com
official hostname: cisco.com
         address: 192.168.219.25

ServiceEngine#dnslookup 10.0.11.0
official hostname: 10.0.11.0
          address: 10.0.11.0
```

enable

To access privileged EXEC commands, use the **enable** EXEC command.

enable

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

To access privileged EXEC mode from user EXEC mode, use the **enable** command. The **disable** command takes you from privileged EXEC mode to user EXEC mode.

Examples

The following example shows how to access privileged EXEC mode:

```
ServiceEngine>enable
ServiceEngine#
```

Related Commands

disable
exit

end

To exit global configuration mode, use the **end** global configuration command.

end

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global configuration

Usage Guidelines

Use the **end** command to exit global configuration mode after completing any changes to the running configuration. To save new configurations to NVRAM, use the **write** command.

In addition, you can press **Ctrl-Z** to exit global configuration mode.

Examples

The following example shows how to exit global configuration mode:

```
ServiceEngine(config)#end
ServiceEngine#
```

Related Commands

exit

exec-timeout

To configure the length of time that an inactive Telnet or Secure Shell (SSH) session remains open, use the **exec-timeout** global configuration command. To revert to the default value, use the **no** form of this command.

exec-timeout *timeout*

no exec-timeout

Syntax Description

timeout	Timeout in minutes (0–44640).

Defaults

The default is 15 minutes.

Command Modes

Global configuration

Usage Guidelines

A Telnet or SSH session with the SE can remain open and inactive for the interval of time specified by the **exec-timeout** command. When the **exec-timeout** interval elapses, the SE automatically closes the Telnet or SSH session.

Configuring a timeout interval of 0 minutes by entering the **exec-timeout 0** command is equivalent to disabling the session-timeout feature.

Examples

The following example configures a timeout of 100 minutes:

```
ServiceEngine(config)#exec-timeout 100
```

The following example negates the configured timeout of 100 minutes and reverts to the default value of 15 minutes:

```
ServiceEngine(config)#no exec-timeout
```

Related Commands

telnet enable
sshd

exit

To access the EXEC command shell from the global, interface, and debug configuration command shells, use the **exit** command.

exit

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC, global configuration, and interface configuration

Usage Guidelines

Use the **exit** command in any configuration mode to return to EXEC mode. Using this command is equivalent to pressing the **Ctrl-Z** key or entering the **end** command.

The **exit** command issued in the user-level EXEC shell terminates the console or Telnet session. You can also use the **exit** command to exit other configuration modes that are available from the global configuration mode for managing specific features (see the commands marked with a footnote in Table 2-1).

Examples

The following example terminates global configuration mode and returns to the privileged-level EXEC mode:

```
ServiceEngine(config)#exit
ServiceEngine#
```

The following example terminates privileged-level EXEC mode and returns to the user-level EXEC mode:

```
ServiceEngine#exit
ServiceEngine>
```

Related Commands

end

external-ip

To configure up to eight external Network Address Translation (NAT) IP addresses, use the **external-ip** global configuration command. To remove the NAT IP addresses, use the **no** form of this command.

external-ip *ip-addresses*

no external-ip *ip-addresses*

Syntax Description

ip-addresses	A maximum of eight external or NAT IP addresses can be configured.

Defaults

No default behavior or values.

Command Modes

Global configuration

Usage Guidelines

Use this command to configure up to eight Network Address Translation IP addresses to allow the router to translate up to eight internal addresses to registered unique addresses and translate external registered addresses to addresses that are unique to the private network. If the IP address of the RTSP gateway has not been configured on the SE, then the external IP address is configured as the IP address of the RTSP gateway.

In an CDS network, there are two methods for a device registered with the CDSM (SEs, SRs, or the standby CDSM) to obtain configuration information from the primary CDSM. The primary method is for the device to periodically poll the primary CDSM on port 443 to request a configuration update. You cannot configure this port number. The backup method is when the CDSM pushes configuration updates to a registered device as soon as possible by issuing a notification to the registered device on port 443. This method allows changes to take effect in a timelier manner. You cannot configure this port number even when the backup method is being used. CDS networks do not work reliably if devices registered with the CDSM are unable to poll the CDSM for configuration updates. When a receiver SE requests the content and content metadata from a forwarder SE, it contacts the forwarder SE on port 443.

When a device (SEs at the edge of the network, SRs, and primary or standby CDSMs) is inside a NAT firewall, those devices that are inside the same NAT use one IP address (the inside local IP address) to access the device and those devices that are outside the NAT use a different IP address (the NAT IP address or inside global IP address) to access the device. A centrally managed device advertises only its inside local IP address to the CDSM. All other devices inside the NAT use the inside local IP address to contact the centrally managed device that resides inside the NAT. A device that is not inside the same NAT as the centrally managed device cannot contact it without a special configuration.

If the primary CDSM is inside a NAT, you can allow a device outside the NAT to poll it for getUpdate requests by configuring a static translation (NAT IP address or inside global IP address) for the CDSM's inside local IP address on its NAT, and using this address, rather than the CDSM's inside local IP address in the **cdsm ip** *ip-address* global configuration command when you register the device to the CDSM. If an SE or SR is inside a NAT and the CDSM is outside the NAT, you can allow the SE or SR to poll for getUpdate requests by configuring a static translation (NAT IP address or inside global IP address) for the SE or SR's inside local address on its NAT.

Note Static translation establishes a one-to-one mapping between your inside local address and an inside global address. Static translation is useful when a host on the inside must be accessible by a fixed address from the outside.

Examples

The following example configures four external NAT IP addresses:

```
ServiceEngine(config)#external-ip 192.168.43.1 192.168.43.2 192.168.43.3 192.168.43.4
```

Related Commands

interface
ip

find-pattern

To search for a particular pattern in a file, use the **find-pattern** EXEC command.

find-pattern {**binary** *filename* | **case** {**binary** *filename* | **count** *filename* | **lineno** *filename* | **match** *filename* | **nomatch** *filename* | **recursive** *filename*} | **count** *filename* | **lineno** *filename* | **match** *filename* | **nomatch** *filename* | **recursive** *filename*}

Syntax Description

binary	Does not suppress the binary output.
filename	Filename.
case	Matches the case-sensitive pattern.
count	Prints the number of matching lines.
lineno	Prints the line number with output.
match	Prints the matching lines.
nomatch	Prints the nonmatching lines.
recursive	Searches a directory recursively.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Use this command to search for a particular regular expression pattern in a file.

Examples

The following example searches a file recursively for a case-sensitive pattern:

```
ServiceEngine#find-pattern case recursive admin removed_core
-rw-------    1 admin    root     95600640 Oct 12 10:27 /local/local1/core_dir/c
ore.2.2.1.b5.eh.2796
-rw-------    1 admin    root     97054720 Jan 11 11:31 /local/local1/core_dir/c
ore.cache.5.3.0.b131.cnbuild.14086
-rw-------    1 admin    root     96845824 Jan 11 11:32 /local/local1/core_dir/c
ore.cache.5.3.0.b131.cnbuild.14823
-rw-------    1 admin    root     101580800 Jan 11 12:01 /local/local1/core_dir/
core.cache.5.3.0.b131.cnbuild.15134
-rw-------    1 admin    root     96759808 Jan 11 12:59 /local/local1/core_dir/c
ore.cache.5.3.0.b131.cnbuild.20016
-rw-------    1 admin    root     97124352 Jan 11 13:26 /local/local1/core_dir/c
ore.cache.5.3.0.b131.cnbuild.30249
-rw-------    1 admin    root     98328576 Jan 11 11:27 /local/local1/core_dir/c
ore.cache.5.3.0.b131.cnbuild.8095
```

The following example searches a file for a pattern and prints the matching lines:

```
ServiceEngine#find-pattern match 10 removed_core
Tue Oct 12 10:30:03 UTC 2004
-rw-------    1 admin    root     95600640 Oct 12 10:27 /local/local1/core_dir/c
ore.5.2.1.b5.eh.2796
-rw-------    1 admin    root     101580800 Jan 11 12:01 /local/local1/core_dir/
core.cache.5.3.0.b131.cnbuild.15134
```

The following example searches a file for a pattern and prints the number of matching lines:

```
ServiceEngine#find-pattern count 10 removed_core
3
```

Related Commands

cd
dir
ls
lls

flash-media-streaming

To enable and configure Flash Media Streaming, use the **flash-media-streaming** global configuration command. To disable Flash Media Streaming, use the **no** form of this command.

On the SE:

flash-media-streaming {**admin-api** [**ip** {**allow** *ip address*}] | **application-virtual-path vod map** *mapping string* | **enable** | **max-bandwidth** *number* | **max-sessions** *number* | **monitoring enable** | **non-wholesale-license-bandwidth** *number* | **wholesale-license** {**install** *number* **license-name** *name* **bandwidth** *number* **start-date** *date* **duration** *number* | **no-alerts** *number*}}

no flash-media-streaming

On the SR:

flash-media-streaming {**enable** | **monitoring enable**}

no flash-media-streaming

Syntax Description

admin-api	Allows accessing admin API from the IP.
ip	Allows an IP Address.
allow	Allows an IP Address
ip address	IP Address or hostname (input maximum 32 of partial or full IP address or hostname, such as 10.60, 10.60.1.133, or foo.com).
application-virtual-path	Configures the virtual-path for applications.
vod	Configures the virtual-path for VOD applications.
map	Maps to a directory.
mapping string	Mapping string.
enable	Enables Flash Media Streaming.
max-bandwidth	Configures Max-bandwidth for Flash Media streaming.
number	Max-bandwidth number (1000–8000000) Kbps.
max-sessions	Configures maximum sessions for Flash Media Streaming.
number	Maximum sessions number (1–15000).
monitoring	Configures Flash Media Streaming monitoring.
enable	Enables monitoring.
non-wholesale-license-bandwidth	Configures non-wholesale-license-bandwidth for Flash Media Streaming.
number	Non-wholesale-license-bandwidth number (1000–8000000) Kbps.
wholesale-license	Adds, modifies, and configures Flash Media Streaming wholesale licenses.
install	Installs wholesale licenses for Flash Media Streaming.
number	License sequence number (1–200).
license-name	Specifies the wholesale license name.
name	Name of the wholesale license.
bandwidth	Specifies the bandwidth of the wholesale license purchased.

number	Wholesale license bandwidth number (1000–4000000) Kbps.
start-date	Specifies the start date of the wholesale license.
date	The start date of the wholesale license in mm-dd-yyyy format, year between 1970 and 2037.
duration	Specifies the duration of the wholesale license, at least 1 month.
number	Duration of the wholesale license.
no-alerts	Disables alerts for Flash Media Streaming wholesale licenses.
number	License sequence number (1–200).
enable	Enables Flash Media Streaming.
monitoring	Configures Flash Media Streaming monitoring.
enable	Enables monitoring.

Defaults

No default behavior or values.

Command Modes

Global configuration

Usage Guidelines

Flash Media Streaming needs an application name (vod, live or dvrcast) as part of a client’s request. In the case of a VOD application, the origin server should have a first level directory of “vod” for dynamic ingestion. For example, in a Flash Media Streaming VOD cache miss case, the request from the client should be rtmp://cdnsecure.bbc.co.uk/vod/iplayerstreaming/secure_auth/scifi.flv, and the origin server should have http://cdnsecure.bbc.co.uk/vod/iplayerstreaming/secure_auth/scifi.flv. However, this restricts customer deployments when “vod” is the only folder name they can use. Therefore, Cisco Internet Streamer Release 2.4 software contains an **application-virtual-path vod** command so customers can map to whichever folder they want on the origin server.

Note The dvrcast option will be available until the 2.4.3 release.

For VOD streams, all RTMP calls in the SWF file must be in the following format:

```
rtmp://rfqdn/vod/path/foo.flv
```

In this format, *rfqdn* is the routing domain name of the Service Router, vod is the required directory, and *path* is the directory path to the content file that conforms to the standard URL specification.

If you are unable to store the VOD content in the required “vod” directory on your origin server, you can create a VOD virtual path for all RTMP requests. All client requests for RTMPcalls still use the rtmp://rfqdn/vod/path/foo.flv format for VOD streams, but the SE replaces the “vod” directory with the string specified in the **flash-media-streaming application-virtual-path vod map** command.

Use the f**lash-media-streaming application-virtual-path vod map <mapping string>** command on each SE participating in a Flash Media Streaming delivery service. The mapping string variable accepts all alpha-numeric characters and the slash (/) character, and can be from 1 to 128 characters. For example, to map the “vod” directory to “media” for the go-tv-stream.com origin server, use the **flash-media-streaming application-virtual-path vod map media** command. If comedy.flv is the content being requested, the RTMP call in the SWF file would be rtmp://go-tv-stream.com/vod/

comedy.flv. The SE would replace the “vod” directory and request http://go-tv-stream.com/media/comedy.flv from the upstream SE or origin server. If just the slash (/) character is used to replace the “vod” directory, the SE request would be http://go-tv-stream.com/comedy.flv.

Editing a Wholesale License

The wholesale license feature has four operations from the CLI—adding and removing licenses and enabling and disabling alerts. Users read license details from the documentation and add them to the CLI and CDSM. If a user enters a license incorrectly, the only way to edit it is to delete the license and add the it again.

Examples

The following example shows how to map a vod folder:

```
ServiceEngine(config)#flash-media-streaming application-virtual-path vod map media
```

This means mapping vod folder to media. When client request cache-miss case: rtmp://Tem4.se.cdsfms.com/vod/foo.flv, will be mapped to rtmp://Temp4.se.cdsfms.com/media/foo.flv

```
ServiceEngine(config)#flash-media-streaming application-virtual-path vod map /
```

This means mapping vod folder to /.

When client request cache-miss case: rtmp://Tem4.se.cdsfms.com/vod/abc/foo.flv, will be mapped to rtmp://Temp4.se.cdsfms.com/abc/foo.flv

When client request cache-miss case: rtmp://Tem4.se.cdsfms.com/vod/bar/foo.flv, will be mapped to rtmp://Temp4.se.cdsfms.com/bar/foo.flv.

show flash-media-streaming
show statistics flash-media-streaming

help

To obtain online help for the command-line interface, use the **help** EXEC or global configuration command.

help

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC and global configuration.

Usage Guidelines

You can get help at any point in a command by entering a question mark (**?**). If nothing matches, the help list will be empty, and you must back up until entering a **?** shows the available options.

Two styles of help are provided:

- Full help is available when you are ready to enter a command argument (for example, **show ?**). In addition, full help describes each possible argument.
- Partial help is provided when you enter an abbreviated command and you want to know what arguments match the input (for example, **show stat?**).

Examples

The following example shows the output of the **help** EXEC command:

```
ServiceEngine#help
Help may be requested at any point in a command by entering a question mark '?'.
Two styles of help are provided:
1. Full help is available when you are ready to enter a command argument.
2. Partial help is provided when an abbreviated argument is entered.
```

hostname

To configure the device’s network hostname, use the **hostname** global configuration command. To reset the hostname to the default setting, use the **no** form of this command.

hostname *name*

no hostname

Syntax Description

name	New hostname for the device; the name is case sensitive. The name may be from 1 to 30 alphanumeric characters.

Defaults

The default hostname is the SE model number.

Command Modes

Global configuration

Usage Guidelines

Use this command to configure the hostname for the SE. The hostname is used for the command prompts and default configuration filenames. This name is also used by content routing and conforms to the following rules:

- It can use only alphanumeric characters and hyphens (-).
- The maximum length is 30 characters.
- The following characters are considered illegal and cannot be used when naming a device: @, #, $,%, ^, &, *, (), |, \””/, <>.

Examples

The following example changes the hostname to Sandbox:

```
ServiceEngine(config)#hostname Sandbox
Sandbox(config)#
```

The following example removes the hostname:

```
ServiceEngine(config)#no hostname
NO-HOSTNAME(config)#
```

Related Commands

dnslookup
ip
show hosts

http

To configure HTTP-related parameters, use the **http** global configuration command. To disable HTTP related-parameters, use the **no** form of this command.

http add-cookie *string*

http age-multiplier *num*

http cache-cookies

http cache-fill-range

http cache-on-abort {**enable** | **percent** *num*}

http max-ttl {**days** *num* | **hours** *num* | **minutes** *num* | **seconds** *num*}

http min-ttl *minutes*

http object max-size *maxsize*

http proxy {**incoming** *ports* | **outgoing** {**host** {*hostname* | *ip-address*} *port*}}

http reval-each-request all

no http

Syntax Description

add-cookie	Add a cookie to going HTTP requests to the origin server.
string	Specifies string to be set as the cookie.
age-multiplier	Specifies the HTTP caching heuristic modifiers.
num	Expiration time of text objects as a percentage of their age (0–100).
cache-cookies	Caches the web objects with associated cookies.
cache-fill-range	Completes cache-fill for a range request starting from 0.
cache-on-abort	Sets the cache-on-abort configuration options.
enable	Enables the cache-on-abort feature.
percent	Sets the percent threshold.
num	Percentage value (1–99).
max-ttl	Sets the maximum Time To Live for objects in the cache.
days	Sets the maximum Time To Live for units in days.
num	Maximum time to live (1–1825).
hours	Sets the maximum Time To Live for units in hours.
num	Maximum time to live (1–43800).
minutes	Sets the maximum Time To Live for units in minutes.
num	Maximum time to live (1–2628000).
seconds	Sets the maximum Time To Live for units in seconds.
num	Maximum time to live (1–157680000).
min-ttl	Sets the minimum Time To Live for objects in the cache.

minutes	Minimum Time To Live in minutes (0–86400).
object	Configures HTTP objects.
max-size	Maximum size of a cacheable object in MBytes, 0 means no limit (0–2047).
maxsize	Maximum size of a cacheable object in kilobytes (1–2096128).
proxy	Configures the incoming proxy-mode requests.
incoming	Configures for incoming proxy-mode requests.
ports	Ports on which to listen for incoming HTTP, FTP, and HTTPS proxy requests (1–65535). You can specify a maximum of eight ports. The default is no incoming proxy.
outgoing	Configures the direct outgoing requests to another proxy server.
host	Uses the outgoing HTTP proxy.
hostname	Hostname of the outgoing proxy.
ip-address	IP address of the outgoing proxy.
port	Port number of the outgoing proxy (1–65535).
reval-each-request	Configures the revalidation for every request.
all	Revalidates all objects on every request.

Defaults

age-multiplier: 30 percent for text objects and 60 percent for binary objects

ports: no incoming proxy

days: 1 day

hours: 24 hours.

minutes: 1440 minutes.

seconds: 86400 seconds.

misses *number*: 0 misses

object max-size: 2 GB

outgoing monitor: 60 seconds

The SE strips the hop-to-hop 407 response sent by the Internet proxy by default.

http cache-on-abort: disabled

The default is no incoming proxy.

Command Modes

Global configuration

Usage Guidelines

Use these commands to configure specific parameters for caching HTTP objects.

Note Text objects refer to HTML pages. Binary objects refer to all other web objects (for example, GIFs or JPEGs).

Transaction Logging

Once a user has been authenticated through LDAP or a RADIUS server, all transaction logs generated by the SE for that user contain user information. If the SE is acting in proxy mode, the user ID is included in the transaction logs. If the SE is acting in transparent mode, the user IP address is included instead.

The **cache-cookies** option enables the SE to cache the binary content served with HTTP Set-cookie headers and no explicit expiration information.

The **reval-each-request** option enables the SE to revalidate all objects requested from the cache.

Use the **object max-size** option to specify the maximum size in kilobytes of a cacheable object. The default is no maximum size for a cacheable object. The **no** form of the command resets the default value.

The **http proxy** options enable the SE to operate in environments where client browsers have previously been configured to use a legacy proxy server. The SE accepts proxy-style requests when the incoming proxy ports are configured with the **http proxy incoming** *ports* option. Up to eight incoming proxy ports can be specified on a single command line or on multiple command lines.

To configure the SE to direct all HTTP miss traffic to a parent cache (without using ICP), use the **http proxy outgoing host** *port* option, where **host** is the system name or IP address of the outgoing proxy server, and *port* is the port number designated by the outgoing (upstream) server to accept proxy requests.

Caching Policy for Client-Aborted Downloads

Typically, a client aborts a download of an object by clicking the **Stop** icon on the browser or by closing the browser during a download. By default, the SE continues to download an object to the cache even after a client aborts the download.

The **cache-on-abort** option lets you specify if and when the SE completes the download of a cacheable object after the client aborts the request. However, if the SE determines that there is another client currently requesting the same object, caching is always completed.

If the **cache-on-abort** option is enabled and no thresholds are enabled, the SE always aborts downloading an object to the cache. You can use any combination of the following thresholds, which are specified in the HTTP header. If the option is not enabled, the client receives an error response. Response errors and read errors are returned to the client, because it is not possible to detect whether these errors are generated at the origin server or at the proxy.

Examples

The following example specifies that the host 10.1.1.1 on port 8088 is designated as the primary proxy server and host 10.1.1.2 is designated as a backup proxy server:

```
ServiceEngine(config)#http proxy outgoing host 10.1.1.1 8088 primary
ServiceEngine(config)#http proxy outgoing host 10.1.1.2 220
```

The following example shows the output for the **show http proxy** command:

```
ServiceEngine#show http proxy
Incoming Proxy-Mode:
  Servicing Proxy mode HTTP connections on ports:   8080

Outgoing Proxy-Mode:
  Primary proxy server: 172.16.63.150   port 1 Failed
  Backup proxy servers: 172.16.236.151  port 8005
                        172.16.236.152  port 123
                        172.16.236.153  port 65535 Failed
                        172.16.236.154  port 10
Monitor Interval for Outgoing Proxy Servers is 60 seconds
Use of Origin Server upon Proxy Failures is disabled.
```

The following example shows the output for the **show statistics http requests** command:

```
ServiceEngine#show statistics http requests
Statistics - Requests
                                                Total             % of Requests
                            ---------------------------------------------------
     Total Received Requests:                   49103                         -
              Forced Reloads:                     109                       0.2
               Client Errors:                      23                       0.0
               Server Errors:                     348                       0.7
                 URL Blocked:                       0                       0.0
      Sent to Outgoing Proxy:                       0                       0.0
Failures from Outgoing Proxy:                       0                       0.0
Excluded from Outgoing Proxy:                       0                       0.0
             ICP Client Hits:                       0                       0.0
             ICP Server Hits:                       0                       0.0
           HTTP 0.9 Requests:                       2                       0.0
           HTTP 1.0 Requests:                   49101                     100.0
           HTTP 1.1 Requests:                       0                       0.0
       HTTP Unknown Requests:                       0                       0.0
           Non HTTP Requests:                       0                       0.0
          Non HTTP Responses:                      46                       0.1
      Chunked HTTP Responses:                       0                       0.0
        Http Miss Due To DNS:                       0                       0.0
     Http Deletes Due To DNS:                       0                       0.0
  Objects cached for min ttl:                    2674                       5.0
```

The following example shows the output for the **show statistics http proxy outgoing** command:

```
ServiceEngine#show statistics http proxy outgoing

HTTP Outgoing Proxy Statistics
IP               PORT    ATTEMPTS   FAILURES
---------------------------------------------------
172.16.23.150    8000    0          0
172.16.23.151    8080    0          0
172.16.23.152    9000    0          0
172.16.23.153    9001    0          0
172.16.23.154    9005    0          0

Requests when all proxies were failed: 0
```

The following example shows that with the default configuration (all **cache-on-abort** thresholds disabled), client abort processing is configured to always abort downloading an object to the cache:

```
ServiceEngine(config)#http cache-on-abort enable
```

The following example shows that the SE is configured to always continue downloading an object to the cache (this configuration is the default):

```
ServiceEngine(config)#no http cache-on-abort
```

The following example shows that the SE is configured to use the default minimum threshold when the **cache-on-abort** option has been enabled and the threshold is set to 16 kilobytes:

```
ServiceEngine(config)#http cache-on-abort min 16
```

The following example shows that the SE is configured to ignore the minimum threshold:

```
ServiceEngine(config)#no http cache-on-abort min
```

Related Commands

acquirer (EXEC mode)
dnslookup
ip name-server
show acquirer
show http
show http proxy
show statistics http requests

icap

To use the Internet Content Adaptation Protocol (ICAP) to help the SE interact with third-party software applications and plug-ins, use the **icap** global configuration command. To disable individual options, use the **no** form of this command.

Note See the "icap service" section on page 2-118 for information about configuring specific ICAP services.

icap {**append-x-headers** {**x-client-ip** | **x-server-ip**} | **apply rules-template** | **service camiant** {**enable** | **error-handling** {**bypass** | **return-error**} | **server** *url*}

no icap {**append-x-headers** {**x-client-ip** | **x-server-ip**} | **apply rules-template** | **service camiant** {**enable** | **error-handling** {**bypass** | **return-error**} | **server** *url*}

Syntax Description

append-x-headers	Appends x-headers during the ICAP protocol handshake. Disabled by default. Can have multiple entries for various x-headers to be appended.
x-client-ip	Appends x-client-IP headers to the request that is sent to the ICAP server. Disabled by default.
x-server-ip	Appends x-server-IP headers to the request that is sent to the ICAP server. Disabled by default.
apply	Enables ICAP processing for HTTP requests.
rules-template	Enables ICAP processing for HTTP requests that match the **rule action use-icap-service** global configuration command.
service	Configures ICAP service.
camiant	Policy server for QoS.
enable	Enables ICAP service.
error-handling	Specifies the error handling option for this service.
bypass	Bypasses this service.
return-error	Returns the error to the client and ends the request.
server	Specifies the server for this service.
url	Specifies the server URL for the style.

Command Modes

Global configuration

Usage Guidelines

ICAP is an open standard for content adaptation, typically at the network edge. Content adaptation is the process of modifying the content to improve its usability. The content adaptation can include virus scanning, content translation, content filtering, content insertion, and other ways of improving the value of content for end users. ICAP specifies how an SE, acting as an HTTP proxy server, can communicate with an external device acting as an ICAP server, which filters and adapts the requested content.

ICAP provides two content-processing modes for HTTP services. These modes define the transactions that can occur between an SE acting as an ICAP client and an ICAP server. The two modes are as follows:

- Request modification (reqmod)—Allows modification of requests as they are sent from the SE to the ICAP server on their way to the origin server. The ICAP server can modify these requests depending on the services requested.
- Response modification (respmod)—Allows modification of requests after they return from the origin server. The ICAP server only acts on requested objects, after they return from the origin server.

The following is a complete list of the ICAP vendors that have been certified to interoperate with the SE:

- TrendMicro for reqmod and respmod
- Symantec for respmod

The maximum file size that is supported in the Internet Streamer CDS software is 2 GB. Files that exceed this size limit are not supported for ICAP processing.

Use the **icap append-x-headers** global configuration command to specify the ICAP extension headers that are passed to the ICAP server during the session negotiation between the SE and the ICAP server as follows:

- You can configure the SE to append the client and server IP address headers to the request that is passed to the ICAP server. This capability allows you to use your ICAP server to perform URL filtering based on the client IP address and server IP address. To enable this capability, you must use the **icap append-x-headers x-client-ip** and **icap append-x-headers x-server-ip** command options.
- You can configure the SE to append the username and group name headers to the request that is passed to the ICAP server. This capability allows you to use your ICAP server to perform URL filtering based on username and group name.

Also, you can choose to apply ICAP services on all HTTP requests processed by the SE or apply ICAP processing only to requests that match the Rules Template. Use the **icap apply** {**all** | **rules-template**} global configuration command to specify which ICAP services should be performed on which requests that are received by the SE. For example, use the **icap apply rules-template** global configuration command to instruct the SE to run only the ICAP services that match the rules action **use-icap-service**. Alternatively, you could use the **icap apply all** global configuration command to instruct the SE to run all of the ICAP services on all of the HTTP requests that it receives.

To exclude other traffic from ICAP processing, use the **rule action use-icap-service** command. The Rules Template can be used to turn off ICAP processing for various requests by applying the patterns available in the Rules Template to the incoming request. These patterns can include the following attributes of the incoming request:

- User-agent field
- Destination IP address
- Domain name

Use the **icap service** command to enter ICAP configuration mode and to configure a specific ICAP service.

Examples

The following example applies ICAP processing to all traffic:

```
ServiceEngine(config)#icap apply all
```

The following examples exclude intranet traffic from ICAP processing:

```
ServiceEngine(config)#rule pattern-list 1 domain !cisco.com
ServiceEngine(config)#rule action use-icap-service trend-reqmod 1 protocol all
ServiceEngine(config)#rule action use-icap-service trend-respmod 1 protocol all
ServiceEngine(config)#rule enable
ServiceEngine(config)#icap apply rules-template
```

The following example shows how to use the **icap service** *service-id* global configuration command to configure and enable various ICAP services on this SE:

```
ServiceEngine(config)#icap service trend-reqmod
ServiceEngine(config-icap-service)#enable
ServiceEngine(config-icap-service)#vector-point reqmod-precache
ServiceEngine(config-icap-service)#server icap//172.19.227.150/REQ-Service
ServiceEngine#exit

ServiceEngine(config)#icap service trend-respmod
ServiceEngine(config-icap-service)#enable
ServiceEngine(config-icap-service)#vector-point respmod-precache
ServiceEngine(config-icap-service)#server icap//172.19.227.150/interscan
ServiceEngine#exit
```

Related Commands

icap service
rule use-icap-service
show icap
show icap service
show rule action use-icap-service

icap service

To enter ICAP service configuration mode and configure ICAP services, enter the **icap service** global configuration command. To disable individual options, use the **no** form of this command.

icap service camiant {**enable** | **error-handling** {**bypass** | **return-error**} | **server** *url*}

no icap service camiant {**enable** | **error-handling** {**bypass** | **return-error**} | **server** *url*}

Syntax Description

camiant	Sets the Policy Server for QoS.
enable	Enables ICAP service.
error-handling	Specifies error-handling option for this service.
bypass	Bypasses this service.
return-error	Returns error to client and end request.
server	Configures servers for this service (1 or more).
url	Server URL of style.

Defaults

server *url*: Port 1344 is assumed if no explicit port is included in the URL.

Command Modes

Global configuration

Usage Guidelines

An ICAP service defines attributes that define the service and one or more servers that provide ICAP services. You can configure a maximum of ten ICAP services on a single SE and a maximum of five ICAP servers for each ICAP service. To select the type of load balancing to use among a cluster of ICAP servers, use the **load-balancing** option.

In the syntax, replace *service-id* with a name of your choice for the current ICAP service. When you enter the **icap service** command and provide a name for the ICAP service, the system displays this ICAP service configuration prompt:

```
ServiceEngine(config-icap-service)#
```

Within ICAP service configuration mode, all commands that you enter apply to the current ICAP service. To return to global configuration mode, enter the **exit** command.

The point at which ICAP services are applied to content is called the *vectoring point*, specified using the **vector-point** option. The following three vectoring points are supported:

- Client request vectoring point (**reqmod-precache**)—The ICAP server performs one of the following actions in response to the client request:
  - Terminates the connection
  - Sends a modified error response
  - Searches the cache using the URL in the request
  - Searches the cache using a modified URL
  - Modifies the request header or request body in the case of a cache miss

- Cache miss vectoring point (**reqmod-postcache**)—The ICAP server performs one of the following actions before forwarding the request to the origin server:
  - Terminates the connection
  - Sends a modified error response
  - Sends the request to the origin server using the original URL
  - Sends the request to the origin server using an alternative URL
  - Modifies the request header or request body
- Server response vectoring point (**respmod-precache**)—The ICAP server performs one of the following actions after receiving the response from the origin server:
  - Returns the response to the client
  - Modifies the request header or request body
  - Caches the response using the original URL
  - Caches the response using an alternative URL

With the **respmod** vectoring point, which is used by virus-scanning ICAP vendors, the performance of the SE will be 300 transactions per second.

With the **reqmod-precache** vectoring point, which is used by URL filtering ICAP vendors, the performance of the SE will drop 20 percent from the rated performance.

Note The performance of the SE will be limited by the performance of the ICAP server.

Note Different ICAP services assigned to the same vectoring point can use different load-balancing options.

ICAP servers process HTTP requests from clients based on the ICAP services configured at various vectoring points. ICAP servers perform content adaptation such as a request or response modification and filtering of requests or responses at the configured vectoring points while processing HTTP requests.

You can configure the maximum number of connections and the weight that can be handled by an ICAP server in a cluster of servers. The weight parameter represents the load percentage that can be redirected to the ICAP server. An ICAP server with a weight of 40 denotes that this server handles 40 percent of the load. If the total weight of all ICAP servers in a load-balanced cluster exceeds 100, the load percentage for each ICAP server is recalculated as a percentage measure represented by the weight parameters.

Note Always locate the ICAP server on a public LAN and configure its public IP address on the SE. The ICAP server should not be located behind a NAT device.

ICAP servers configured at various vectoring points (especially the request modification precache vectoring points) may become overloaded with HTTP requests, because all requests pass through this point. Therefore, a cluster of ICAP servers (a load-balanced collection of ICAP servers) is made available for configuration. At a particular vectoring point, you can choose to load balance requests among the ICAP cluster of servers based on various parameters such as weighted load, client IP and server IP address-based hash, or round-robin format.

More than one ICAP service can be associated with a vectoring point. An ICAP service configured at a vectoring point can have only one load-balancing scheme, irrespective of the number of servers. However, multiple ICAP services configured at one or all of the vectoring points can have different load-balancing schemes.

To identify the specific ICAP server and service, use the **server** *url* command, where the URL is in the following format:

icap://*ICAPserverIPaddress/service-name*

The value used for the *service-name* must match the identifier used by the specific ICAP vendor. For example, one vendor uses the service name REQ-Service for **reqmod-precache** and interscan for **respmod-precache**, while another vendor supports only **respmod-precache** and uses the service name avscan.

When ICAP processing is enabled and an HTTP browser with a streaming Java applet is opened, several undesirable things occur as follows:

- The data for the Java applet is not updated in the browser. For example, when viewing a stock investment website, a user would not see any streaming stock updates.
- The ICAP daemon on the SE continues to send updates (from the HTTP response) to the ICAP server, which overloads the ICAP server.

These conditions occur because the ICAP server is set up to inspect the entire data packet before delivering a response to the client. However, because there is a streaming request, the data continues flowing to the ICAP server indefinitely, deadlocking any response to the requesting client.

Two workarounds are available. You can configure the ICAP server to bypass the scanning process, or you can configure rules on the SE to skip ICAP processing on websites that are known to contain streaming Java applets.

To configure the ICAP server to bypass scanning, use rules such as client_skip_content or server_skip_content as follows:

- The client_skip_content rule bypasses scanning on the basis of an HTTP request. The software looks for patterns in the HTTP header and bypasses all requests that exactly match the patterns specified in the intscan.ini file as follows:

  ```
  client_skip_content=User Agent: Windows Media Player 9.0.1
  ```

- The server_skip_content rule bypasses scanning on the basis of an HTTP response. The software looks for patterns in the HTTP header and bypasses all responses that exactly match the patterns specified in the intscan.ini file as follows:

  ```
  server_skip_content=Content-Type: X-Dave_Content
  ```

Alternatively, you can configure the SE to bypass ICAP processing based on user agents or any of the patterns available in the Rules Template, by using the **rule** command.

Examples

The following examples show a typical configuration for a virus scanning service that requires processing on two vectoring points (**reqmod-precache** and **respmod-precache**):

```
ServiceEngine(config)#icap apply all
ServiceEngine(config)#icap service trend-reqmod
ServiceEngine(config-icap-service)#enable
ServiceEngine(config-icap-service)#vector-point reqmod-precache
ServiceEngine(config-icap-service)#server icap://172.19.227.150/REQ-Service
ServiceEngine#exit
ServiceEngine#icap service trend-respmod
ServiceEngine(config-icap-service)#enable
```

```
ServiceEngine(config-icap-service)#vector-point respmod-precache
ServiceEngine(config-icap-service)#server icap://172.19.227.150/interscan
ServiceEngine#exit
```

The following example shows that if an ICAP vendor supports the same service name for more than one vectoring point, you can configure a single service and add the supported vectoring points:

```
ServiceEngine(config)#icap service myicap-service
ServiceEngine(config-icap-service)#enable
ServiceEngine(config-icap-service)#vector-point reqmod-precache
ServiceEngine(config-icap-service)#vector-point respmod-precache
ServiceEngine(config-icap-service)#server icap://172.19.227.150/icap-service-name
ServiceEngine(config-icap-service)#exit
ServiceEngine(config)#
```

The following example shows that the SE is configured to bypass ICAP processing on the intranet site cisco.com and on the trusted Internet site datek.com:

```
SE(config)#rule enable
SE(config)#rule action use-icap-service trend-reqmod pattern-list 1 protocol all
SE(config)#rule action use-icap-service trend-respmod pattern-list 1 protocol all
SE(config)#rule pattern-list 1 domain !(.*cisco\.com|.*datek\.com)!
SE(config)#icap apply rules-template
SE(config)#icap service trend-reqmod
SE(config-icap-service)#enable
SE(config-icap-service)#vector-point reqmod-precache
SE(config-icap-service)#server icap://172.19.227.150/REQ-Service
SE(config-icap-service)#exit
SE(config)#icap service trend-respmod
SE(config-icap-service)#enable
SE(config-icap-service)#vector-point respmod-precache
SE(config-icap-service)#server icap://172.19.227.150/interscan
SE(config-icap-service)#exit
```

Related Commands

icap
rule use-icap-service
show icap
show icap service
show rule action use-icap-service

install

To install the Internet Streamer CDS software image, use the **install** EXEC command.

install *imagefilename*

Syntax Description

imagefilename	Name of the .bin file that you want to install.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

The **install** command loads the system image into flash memory and the disk.

To install a system image, copy the image file to the sysfs directory local1 or local2. Before entering the **install** command, change the present working directory to the directory where the system image resides. When the **install** command is executed, the image file is expanded. The expanded files overwrite the existing files in the SE. The newly installed version takes effect after the system image is reloaded.

Note The **install** command does not accept .pax files. Files should be of the .bin type (for example, CDS-2.2.1.7-K9.bin). Also, if the release being installed does not require a new system image, then it may not be necessary to write to flash memory. If the newer version has changes that require a new system image to be installed, then the **install** command may result in a write to flash memory.

Examples

The following example shows how to install a .bin file on the SE:

```
ServiceEngine#install CDS-2.2.1.7-K9.bin
```

Related Commands

copy ftp install
copy http install
reload

interface

To configure a Gigabit Ethernet or port-channel interface, use the **interface** global configuration command. To disable selected options, restore default values, or enable a shutdown interface, use the **no** form of this command.

interface GigabitEthernet *slot/port*

interface PortChannel {**1** | **2**}

interface standby *group number*

no interface {**GigabitEthernet** *slot/port* | **PortChannel** {**1** | **2**} | **Standby** *group number*}

Syntax Description

GigabitEthernet	Selects a Gigabit Ethernet interface to configure.
slot/port	Slot and port number for the selected interface. The slot range is 0–12; the port range is 0–0. The slot number and port number are separated with a forward slash character (/).
PortChannel	Selects the EtherChannel of interfaces to configure.
1	Sets the port-channel interface number to 1.
2	Sets the port-channel interface number to 2.
Standby	Sets the standby group for the interface.
group number	Group number for the selected interface. The group number range is 1–4.

Defaults

No default behavior or values.

Command Modes

Global configuration

Usage Guidelines

Configuring Interfaces for DHCP

During the initial configuration of an SE, you have the option of configuring a static IP address for the SE or using interface-level DHCP to dynamically assign IP addresses to the interfaces on the SE.

If you do not enable interface-level DHCP on the SE, you must manually specify a static IP address and network mask for the SE. If the SE moves to another location in another part of the network, you must manually enter a new static IP address and network mask for this SE.

An interface can be enabled for DHCP by using the **ip address dhcp** [*client_id* | *hostname*] interface configuration command. The client identifier is an ASCII value. The SE sends its configured client identifier and hostname to the DHCP server when requesting network information. DHCP servers can be configured to identify the client identifier information and the hostname information that the SE is sending and then send back the specific network settings that are assigned to the SE.

String to Be Set as Cookie Port-Channel (EtherChannel) Interface

EtherChannel for the Internet Streamer CDS Release 2.x software supports the grouping of up to four same- network interfaces into one virtual interface. This grouping allows the setting or removing of a virtual interface that consists of two Gigabit Ethernet interfaces. EtherChannel also provides interoperability with Cisco routers, switches, and other networking devices or hosts supporting EtherChannel, load balancing, and automatic failure detection and recovery based on each interface's current link status.

You can use the Gigabit Ethernet ports to form an EtherChannel. A physical interface can be added to an EtherChannel subject to the device configuration.

Examples

The following example creates an EtherChannel. The port channel is port channel 2 and is assigned an IP address of 10.10.10.10 and a netmask of 255.0.0.0:

```
ServiceEngine# configure
ServiceEngine(config)# interface PortChannel 2
ServiceEngine(config-if)# exit
```

The following example removes an EtherChannel:

```
ServiceEngine(config)# interface PortChannel 2
ServiceEngine(config-if)# exit
ServiceEngine(config)# no interface PortChannel 2
```

The following example shows a sample output of the **show running-config** EXEC command:

```
ServiceEngine# show running-config
.
.
.
interface GigabitEthernet 0/0
 description This is an interface to the WAN
 ip address dhcp
 ip address 192.168.1.200 255.255.255.0
bandwidth 100
exit
.
.
```

The following example shows the sample output of the **show interface** command:

```
ServiceEngine# show interface GigabitEthernet 1/0
Description: This is the interface to the lab
type: Ethernet
```

The following example shows how to create standby groups on SEs:

```
ServiceEngine(config)#interface GigabitEthernet 1/0 standby 2 priority 300
ServiceEngine(config)#interface GigabitEthernet 2/0 standby 2 priority 200
ServiceEngine(config)#interface GigabitEthernet 3/0 standby 2 priority 100
ServiceEngine(config)#interface standby 2 errors 10000
```

Related Commands

show interface
show running-config
show startup-config

ip

To change initial network device configuration settings, use the **ip** global configuration command. To delete or disable these settings, use the **no** form of this command. The **dscp** option allows you to set the global Type of Service (ToS) or differentiated services code point (DSCP) values in IP packets.

ip default-gateway *ip-address*

ip domain-name *name1 name2 name3*

ip dscp {**client** {**cache-hit** {**match-server** | **set-dscp** *dscp-packets* | **set-tos** *tos-packets*} | **cache-miss** {**match-server** | **set-dscp** *dscp-packets* | **set-tos** *tos-packets*}} | **server** {**match-client** | **set-dscp** *dscp-packets* | **set-tos** *tos-packets*}}

ip name-server *ip-addresses*

ip path-mtu-discovery enable

ip route *dest_addrs net_addrs gateway_addrs*

no ip {**default-gateway** | **domain-name** | **dscp** {**client** {**cache-hit** | **cache-miss**} | **server**} | **name-server** *ip-addresses* | **path-mtu-discovery enable** | **route** *dest_addrs net_addrs gateway_addrs*}

Syntax Description

default-gateway	Specifies the default gateway (if not routing IP).
ip-address	IP address of the default gateway.
domain-name	Specifies domain names.
name1 through *name3*	Domain name (up to three can be specified).
dscp	Configures IP differentiated services code point (DSCP) and Type of Service (ToS) fields.
client	Configures DSCP for responses to the client.
cache-hit	Configures the cache hit responses to the client.
cache-miss	Configures the cache miss responses to the client.
match-server	Uses the original ToS/DSCP value of the server.
set-dscp	Configures differentiated services code point (DSCP) values.
dscp-packets	DSCP values; see Table 2-6 on page 2-127 for valid values.
set-tos	Configures Type of Service (ToS).
tos-packets	ToS value; see Table 2-8 on page 2-131 for valid values.
server	Configures DSCP for outgoing requests.
match-client	Uses the original ToS/DSP value of the client.
name-server	Specifies the address of the name server.
ip-addresses	IP addresses of the name servers (up to a maximum of eight).
path-mtu-discovery	Configures RFC 1191 Path Maximum Transmission Unit (MTU) discovery.
enable	Enables Path MTU discovery.
route	Specifies the net route.

dest_addrs	Destination route address.
net_addrs	Netmask address.
gateway_addrs	Gateway address.

Defaults

No default behavior or values.

Command Modes

Global configuration

Usage Guidelines

To define a default gateway, use the **ip default-gateway** command. Only one default gateway can be configured. To remove the IP default gateway, use the **no** form of this command. The SE uses the default gateway to route IP packets when there is no specific route found to the destination.

To define a default domain name, use the **ip domain-name** command. To remove the IP default domain name, use the **no** form of this command. Up to three domain names can be entered. If a request arrives without a domain name appended in its hostname, the proxy tries to resolve the hostname by appending *name1*, *name2*, and *name3* in that order until one of these names succeeds.

The SE appends the configured domain name to any IP hostname that does not contain a domain name. The appended name is resolved by the DNS server and then added to the host table. The SE must have at least one domain name server specified for hostname resolution to work correctly.

To specify the address of one or more name servers to use for name and address resolution, use the **ip name-server** *ip-addresses* command. To disable IP name servers, use the **no** form of this command. For proper resolution of the hostname to the IP address or the IP address to the hostname, the SE uses DNS servers. Use the **ip name-server** command to point the SE to a specific DNS server. You can configure up to eight servers.

Path MTU autodiscovery discovers the MTU and automatically sets the correct value. Use the **ip path-mtu-discovery enable** command to start this autodiscovery utility. By default, this feature is enabled. When this feature is disabled, the sending device uses a packet size that is smaller than 576 bytes and the next hop MTU. Existing connections are not affected when this feature is turned on or off.

The Cisco Internet Streamer CDS software supports IP Path MTU Discovery, as defined in RFC 1191. When enabled, Path MTU Discovery discovers the largest IP packet size allowable between the various links along the forwarding path and automatically sets the correct value for the packet size. By using the largest MTU that the links will bear, the sending device can minimize the number of packets that it must send.

Note IP Path MTU Discovery is useful when a link in a network goes down, forcing the use of another, different MTU-sized link. IP Path MTU Discovery is also useful when a connection is first being established and the sender has no information at all about the intervening links.

IP Path MTU Discovery is initiated by the sending device. If a server does not support IP Path MTU Discovery, the receiving device will have no mechanism available to avoid fragmenting datagrams generated by the server.

Use the **ip route** command to add a specific static route for a network or host. Any IP packet designated for the specified destination uses the configured route.

To configure static IP routing, use the **ip route** command. To remove the route, use the **no** form of this command. Do not use the **ip route 0.0.0.0 0.0.0.0** command to configure the default gateway; use the **ip default-gateway** command instead.

In the CDS network, you can configure SEs, SRs, and CDSMs for the Type of Service (ToS) or differentiated services code point (DSCP) using the **ip dscp** command.

Differentiated Services

The differentiated services (DiffServ) architecture is based on a simple model where traffic entering a network is classified and possibly conditioned at the boundaries of the network. The class of traffic is then identified with a differentiated services (DS) code point or bit marking in the IP header. Within the core of the network, packets are forwarded according to the per-hop behavior associated with the DS code point.

To set the global ToS or DSCP values for the IP header from the CLI, use the **ip dscp** command.

DiffServ describes a set of end-to-end QoS (Quality of Service) capabilities. End-to-end QoS is the ability of the network to deliver service required by specific network traffic from one end of the network to another. QoS in the Internet Streamer CDS software supports differentiated services.

With differentiated services, the network tries to deliver a particular kind of service based on the QoS specified by each packet. This specification can occur in different ways, for example, using the 6-bit DSCP setting in IP packets or source and destination addresses. The network uses the QoS specification to classify, mark, shape, and police traffic, and to perform intelligent queueing.

Differentiated services is used for several mission-critical applications and for providing end-to-end QoS. Typically, differentiated services is appropriate for aggregate flows because it performs a relatively coarse level of traffic classification.

Use the **ip dscp** {**client** | **server**} {**cache-hit** | **cache-miss**} **set-dscp** *dscp-packets* command to set the DSCP values for the IP header. Valid values for *dscp-packets* are listed in Table 2-6.

Table 2-6 dscp-packets Values

Value or Keyword	Description[1]
0–63	Sets DSCP values.
af11	Sets packets with AF11 DSCP (001010).
af12	Sets packets with AF12 DSCP (001100).
af13	Sets packets with AF13 DSCP (001110).
af21	Sets packets with AF21 DSCP (010010).
af22	Sets packets with AF22 DSCP (010100).
af23	Sets packets with AF23 DSCP (010110).
af31	Sets packets with AF31 DSCP (011010).
af32	Sets packets with AF32 DSCP (011100).
af33	Sets packets with AF33 DSCP (011110).
af41	Sets packets with AF41 DSCP (100010).
af42	Sets packets with AF42 DSCP (100100).
af43	Sets packets with AF43 DSCP (100110).
cs1	Sets packets with CS1 (precedence 1) DSCP (001000).
cs2	Sets packets with CS2 (precedence 2) DSCP (010000).

Table 2-6 dscp-packets Values (continued)

Value or Keyword	Description[1]
cs3	Sets packets with CS3 (precedence 3) DSCP (011000).
cs4	Sets packets with CS4 (precedence 4) DSCP (100000).
cs5	Sets packets with CS5 (precedence 5) DSCP (101000).
cs6	Sets packets with CS6 (precedence 6) DSCP (110000).
cs7	Sets packets with CS7 (precedence 7) DSCP (111000).
default	Sets packets with the default DSCP (000000).
ef	Sets packets with EF DSCP (101110).

[1] The number in parentheses denotes the DSCP value for each per-hop behavior keyword.

DS Field Definition

A replacement header field, called the DS field, is defined by differentiated services. The DS field supersedes the existing definitions of the IPv4 ToS octet (RFC 791) and the IPv6 traffic class octet. Six bits of the DS field are used as the DSCP to select the Per Hop Behavior (PHB) at each interface. A currently unused (CU) 2-bit field is reserved for explicit congestion notification (ECN). The value of the CU bits is ignored by DS-compliant interfaces when determining the PHB to apply to a received packet.

Per-Hop Behaviors

RFC 2475 defines PHB as the externally observable forwarding behavior applied at a DiffServ-compliant node to a DiffServ Behavior Aggregate (BA).

With the ability of the system to mark packets according to the DSCP setting, collections of packets that have the same DSCP setting and that are sent in a particular direction can be grouped into a BA. Packets from multiple sources or applications can belong to the same BA.

A PHB refers to the packet scheduling, queueing, policing, or shaping behavior of a node on any given packet belonging to a BA, as configured by a service level agreement (SLA) or a policy map.

There are four available standard PHBs as follows:

- Default PHB (as defined in RFC 2474)
- Class-Selector PHB (as defined in RFC 2474)
- Assured Forwarding (AFny) PHB (as defined in RFC 2597)
- Expedited Forwarding (EF) PHB (as defined in RFC 2598)

The following sections describe the PHBs.

Default PHB

The default PHB specifies that a packet marked with a DSCP value of 000000 (recommended) receives the traditional best-effort service from a DS-compliant node (a network node that complies with all of the core DiffServ requirements). Also, if a packet arrives at a DS-compliant node, and the DSCP value is not mapped to any other PHB, the packet gets mapped to the default PHB.

Class-Selector PHB

To preserve backward compatibility with any IP precedence scheme currently in use on the network, DiffServ has defined a DSCP value in the form xxx000, where x is either 0 or 1. These DSCP values are called Class-Selector Code Points. (The DSCP value for a packet with default PHB 000000 is also called the Class-Selector Code Point.)

The PHB associated with a Class-Selector Code Point is a Class-Selector PHB. These Class-Selector PHBs retain most of the forwarding behavior as nodes that implement IP precedence-based classification and forwarding.

For example, packets with a DSCP value of 110000 (the equivalent of the IP precedence-based value of 110) have preferential forwarding treatment (for scheduling, queueing, and so on), as compared to packets with a DSCP value of 100000 (the equivalent of the IP precedence-based value of 100). These Class-Selector PHBs ensure that DS-compliant nodes can coexist with IP precedence-based nodes.

Assured Forwarding PHB

Assured Forwarding PHB is nearly equivalent to Controlled Load Service, which is available in the integrated services model. AFny PHB defines a method by which BAs can be given different forwarding assurances.

For example, network traffic can be divided into the following classes:

- Gold—Traffic in this category is allocated 50 percent of the available bandwidth.
- Silver—Traffic in this category is allocated 30 percent of the available bandwidth.
- Bronze—Traffic in this category is allocated 20 percent of the available bandwidth.

The AFny PHB defines four AF classes: AF1, AF2, AF3, and AF4. Each class is assigned a specific amount of buffer space and interface bandwidth according to the SLA with the service provider or policy map.

Within each AF class, you can specify three drop precedence (dP) values: 1, 2, and 3. Assured Forwarding PHB can be expressed as shown in the following example: AFny. In this example, n represents the AF class number (1, 2, or 3) and y represents the dP value (1, 2, or 3) within the AFn class.

In instances of network traffic congestion, if packets in a particular AF class (for example, AF1) need to be dropped, packets in the AF1 class will be dropped according to the following guideline:

dP(AFny) >= dP(AFnz) >= dP(AFnx)

where dP (AFny) is the probability that packets of the AFny class will be dropped and y denotes the dP within an AFn class.

In the following example, packets in the AF13 class will be dropped before packets in the AF12 class, which in turn will be dropped before packets in the AF11 class:

dP(AF13) >= dP (AF12) >= dP(AF11)

The dP method penalizes traffic flows within a particular BA that exceed the assigned bandwidth. Packets on these offending flows could be re-marked by a policer to a higher drop precedence.

An AFx class can be denoted by the DSCP value, xyzab0, where xyz can be 001, 010, 011, or 100, and ab represents the dP value.

Table 2-7 lists the DSCP value and corresponding dP value for each AF PHB class.

Table 2-7 DSCP Values and Corresponding Drop Precedence Values for Each AF PHB Class

Drop Precedence	Class 1	Class 2	Class 3	Class 4
Low drop precedence	001010	010010	011010	100010
Medium drop precedence	001100	010100	011100	100100
High drop precedence	001110	010110	011110	100110

Expedited Forwarding PHB

Resource Reservation Protocol (RSVP), a component of the integrated services model, provides a guaranteed bandwidth service. Applications, such as Voice over IP (VoIP), video, and online trading programs, require this type of service. The EF PHB, a key ingredient of DiffServ, supplies this kind of service by providing low loss, low latency, low jitter, and assured bandwidth service.

You can implement EF by using priority queueing (PQ) and rate limiting on the class (or BA). When implemented in a DiffServ network, EF PHB provides a virtual leased line or premium service. For optimal efficiency, however, you should reserve EF PHB for only the most critical applications because, in instances of traffic congestion, it is not feasible to treat all or most traffic as high priority.

EF PHB is suited for applications such as VoIP that require low bandwidth, guaranteed bandwidth, low delay, and low jitter.

IP Precedence for ToS

IP precedence allows you to specify the class of service (CoS) for a packet. You use the three precedence bits in the IPv4 header's type of service (ToS) field for this purpose.

Using the ToS bits, you can define up to six classes of service. Other features configured throughout the network can then use these bits to determine how to treat the packet. These other QoS features can assign appropriate traffic-handling policies including congestion management strategy and bandwidth allocation. For example, although IP precedence is not a queueing method, queueing methods such as weighted fair queueing (WFQ) and Weighted Random Early Detection (WRED) can use the IP precedence setting of the packet to prioritize traffic.

By setting precedence levels on incoming traffic and using them with the Internet Streamer CDS software QoS queueing features, you can create differentiated service. You can use features, such as policy-based routing (PBR) and Committed Access Rate (CAR), to set the precedence based on an extended access list classification. For example, you can assign the precedence based on the application or user or by destination and source subnetwork.

So that each subsequent network element can provide service based on the determined policy, IP precedence is usually deployed as close to the edge of the network or the administrative domain as possible. IP precedence is an edge function that allows core or backbone QoS features, such as WRED, to forward traffic based on CoS. You can also set IP precedence in the host or network client, but this setting can be overridden by the service provisioning policy of the domain within the network.

The following QoS features can use the IP precedence field to determine how traffic is treated:

- Distributed-WRED
- WFQ
- CAR

How the IP Precedence Bits Are Used to Classify Packets

You use the three IP precedence bits in the ToS field of the IP header to specify a CoS assignment for each packet. You can partition traffic into up to six classes—the remaining two classes are reserved for internal network use—and then use policy maps and extended ACLs to define network policies in terms of congestion handling and bandwidth allocation for each class.

Each precedence corresponds to a name. These names, which continue to evolve, are defined in RFC 791. The numbers and their corresponding names, are listed from least to most important.

IP precedence allows you to define your own classification mechanism. For example, you might want to assign the precedence based on an application or an access router. IP precedence bit settings 96 and 112 are reserved for network control information, such as routing updates.

The IP precedence field occupies the three most significant bits of the ToS byte. Only the three IP precedence bits reflect the priority or importance of the packet, not the full value of the ToS byte.

Use the **ip dscp** {**client** | **server**} {**cache-hit** | **cache-miss**} **set-tos** *tos-packets* command to specify either of the two arguments—IP precedence or ToS byte value—to set the same ToS. You may specify either the ToS byte value or IP precedence; one is required. IP precedence uses the three precedence bits in the ToS field of the IPv4 header to specify the class of service for each packet. The ToS byte in the IP header defines the three high-order bits as IP precedence bits and the five low-order bits as ToS bits. The ToS byte value is written to the five low-order bits (bits 0 to 4) of the ToS byte in the IP header of a packet. The IP precedence value is written to the three high-order bits (bits 5 to 7) of the ToS byte in the IP header of a packet.

The following is a list of precedence names:

- **critical**
- **flash**
- **flash-override**
- **immediate**
- **internet**
- **network**
- **priority**
- **routine**

The following is a list of ToS names:

- **max-reliability**
- **max-throughput**
- **min-delay**
- **min-monetary-cost**
- **normal**

Valid values for *tos-packets* are listed in Table 2-8.

Table 2-8 tos-packets Values

Value, Precedence, or ToS Name	Description[1]
0–127	Sets the ToS value.
critical	Sets packets with critical precedence (80).
flash	Sets packets with flash precedence (48).
flash-override	Sets packets with flash override precedence (64).
immediate	Sets packets with immediate precedence (32).
internet	Sets packets with internetwork control precedence (96).
max-reliability	Sets packets with maximum reliable ToS (2).
max-throughput	Sets packets with maximum throughput ToS (4).
min-delay	Sets packets with minimum delay ToS (8).
min-monetary-cost	Sets packets with minimum monetary cost ToS (1).
network	Sets packets with network control precedence (112).

Table 2-8 tos-packets Values (continued)

Value, Precedence, or ToS Name	Description[1]
normal	Sets packets with normal ToS (0).
priority	Sets packets with priority precedence (16).

[1] The number in parentheses denotes the ToS value for each IP precedence or ToS name setting.

Examples

The following example configures a default gateway for the SE:

```
ServiceEngine(config)#ip default-gateway 192.168.7.18
```

The following example disables the default gateway:

```
ServiceEngine(config)#no ip default-gateway
```

The following example configures a static IP route for the SE:

```
ServiceEngine(config)#ip route 172.16.227.128 255.255.255.0 172.16.227.250
```

The following example negates the static IP route:

```
ServiceEngine(config)#no ip route 172.16.227.128 255.255.255.0 172.16.227.250
```

The following example configures a default domain name for the SE:

```
ServiceEngine(config)#ip domain-name cisco.com
```

The following example negates the default domain name:

```
ServiceEngine(config)#no ip domain-name
```

The following example configures a name server for the SE:

```
ServiceEngine(config)#ip name-server 10.11.12.13
```

The following example disables the name server:

```
ServiceEngine(config)#no ip name-server 10.11.12.13
```

Related Commands

show ip route

ip access-list

To create and modify access lists for controlling access to interfaces or applications, use the **ip access-list standard** or **ip access-list extended** global configuration commands. To remove access control lists, use the **no** form of this command.

```
ip access-list { extended {acl-name | acl-num {delete num | deny { num { ip address | any | host}
    | gre {ip address | any | host} | icmp{ip address | any | host} | ip {ip address | any | host} | tcp
    {ip address | any | host} | udp {ip address | any | host}} | insert {num {deny | permit} | list
    {start-line-num | end-line-num} | move {old-line-num | new-line-num} | permit {num {ip
    address | any | host} | gre {ip address | any | host} | icmp{ip address | any | host} | ip {ip address
    | any | host} | tcp {ip address | any | host} | udp {ip address | any | host}}} | {standard {acl-num
    | acl-name {delete num | deny {num {ip address | any | host} | gre {ip address | any | host} |
    icmp{ip address | any | host} | ip {ip address | any | host} | tcp {ip address | any | host} | udp
    {ip address | any | host}} | insert {num {deny | permit} | list {start-line-num | end-line-num} |
    move {old-line-num | new-line-num} | permit {ip address | any | host}}}}
```

```
no ip access-list {extended {acl-name | acl-num {delete num | deny {num {ip address | any | host}
    | gre {ip address | any | host} | icmp{ip address | any | host} | ip {ip address | any | host} | tcp
    {ip address | any | host} | udp {ip address | any | host}} | insert {num {deny | permit} | list
    {start-line-num | end-line-num} | move {old-line-num | new-line-num} | permit {num {ip
    address | any | host} | gre {ip address | any | host} | icmp{ip address | any | host} | ip {ip address
    | any | host} | tcp {ip address | any | host} | udp {ip address | any | host}}} | {standard {acl-num
    | acl-name {delete num | deny {num {ip address | any | host} | gre {ip address | any | host} |
    icmp{ip address | any | host} | ip {ip address | any | host} | tcp {ip address | any | host} | udp
    {ip address | any | host}} | insert {num {deny | permit} | list {start-line-num | end-line-num} |
    move {old-line-num | new-line-num} | permit {ip address | any | host}}}}
```

Syntax Description

standard	Enables the standard ACL configuration mode.
acl-num	Access list to which all commands entered from access list configuration mode apply, using a numeric identifier. For standard access lists, the valid range is 1 to 99; for extended access lists, the valid range is 100 to 199.
acl-name	Access list to which all commands entered from ACL configuration mode apply, using an alphanumeric string of up to 30 characters, beginning with a letter.
delete	(Optional) Deletes the specified entry.
num	(Optional) Position of condition to delete (1–500).
deny	(Optional) Causes packets that match the specified conditions to be dropped.
num	An IP Protocol Number.
ip address	Source IP address.
any	Any source host.
host	A single host address.
gre	Cisco's GRE Tunneling.
icmp	Internet Control Message Protocol.
ip	Any IP Protocol.
tcp	Transport Control Protocol.

udp	User Datagram Protocol.
insert	(Optional) Inserts the conditions following the specified line number into the access list.
num	Identifies the position at which to insert a new condition.
deny	Specifies packets to deny.
permit	Specifies packets to permit.
list	(Optional) Lists the specified entries (or all entries when none are specified).
start-line-num	(Optional) Line number from which the list begins.
end-line-num	(Optional) Last line number in the list.
move	(Optional) Moves the specified entry in the access list to a new position in the list.
old-line-num	Line number of the entry to move.
new-line-num	New position of the entry. The existing entry is moved to the following position in the access list.
permit	(Optional) Causes packets that match the specified conditions to be accepted for further processing.
extended	Enables the extended ACL configuration mode.

Defaults

An access list drops all packets unless you configure at least one **permit** entry.

Command Modes

Global configuration

Usage Guidelines

Standard ACL Configuration Mode Commands

To work with a standard access list, enter the **ip access-list standard** command from the global configuration mode prompt. The CLI enters a configuration mode in which all subsequent commands apply to the current access list.

To add a line to the standard IP ACL, enter the following command:

For example, choose a purpose (permit or deny) that specifies whether a packet is to be passed or dropped, enter the source IP address, and enter the source IP wildcard address as follows:

[**insert** *line-num*] {**deny** | **permit**} {*source-ip* [*wildcard*] | **host** *source-ip* | **any**}

To delete a line from the standard IP ACL, enter the following command:

delete *line-num*

To display a list of specified entries within the standard IP ACL, enter the following command:

list [*start-line-num* [*end-line-num*]]

To move a line to a new position within the standard IP ACL, enter the following command:

move *old-line-num new-line-num*

To return to the CLI global configuration mode prompt, enter the following command:

exit

To negate a standard IP ACL, enter the following command:

no {**deny** | **permit**} {*source-ip* [*wildcard*] | **host** *source-ip* | **any**}

Extended ACL Configuration Mode Commands

To work with an extended access list, enter the **ip access-list extended** command from the global configuration mode prompt. The CLI enters a configuration mode in which all subsequent commands apply to the current access list.

To delete a line from the extended IP ACL, enter the following command:

delete *line-num*

To move a line to a new position within the extended IP ACL, enter the following command:

move *old-line-num new-line-num*

To display a list of specified entries within the standard IP ACL, enter the following command:

list [*start-line-num* [*end-line-num*]]

To return to the CLI global configuration mode prompt, enter the following command:

exit

To add a condition to the extended IP ACL, note that the options depend on the chosen protocol.

For IP, enter the following command to add a condition:

[**insert** *line-num*] {**deny** | **permit**}{**gre** | **ip** | *proto-num*} {*source-ip* [*wildcard*] | **host** *source-ip* | **any**} {*dest-ip* [*wildcard*] | **host** *dest-ip* | **any**}

no {**deny** | **permit**}{**gre** | **ip** | *proto-num*} {*source-ip* [*wildcard*] | **host** *source-ip* | **any**} {*dest-ip* [*wildcard*] | **host** *dest-ip* | **any**}

where if you enter *proto-num* is 47 or 0, they represent the equivalent value for GRE or IP.

For TCP, enter the following command to add a condition:

[**insert** *line-num*] {**deny** | **permit**} {**tcp** | *proto-num*} {*source-ip* [*wildcard*] | **host** *source-ip* | **any**} [*operator port* [*port*]] {*dest-ip* [*wildcard*] | **host** *dest-ip* | **any**} [*operator port* [*port*]] [**established**]

no {**deny** | **permit**} {**tcp** | *proto-num*} {*source-ip* [*wildcard*] | **host** *source-ip* | **any**} [*operator port* [*port*]] {*dest-ip* [*wildcard*] | **host** *dest-ip* | **any**} [*operator port* [*port*]] [**established**]

where *proto-num* can be 6, which is the equivalent value for TCP.

For UDP, enter the following command to add a condition:

[**insert** *line-num*] {**deny** | **permit**} {**udp** | *proto-num*} {*source-ip* [*wildcard*] | **host** *source-ip* | **any**} [*operator port* [*port*]] {*dest-ip* [*wildcard*] | **host** *dest-ip* | **any**} [*operator port* [*port*]]

no {**deny** | **permit**} {**udp** | *proto-num*} {*source-ip* [*wildcard*] | **host** *source-ip* | **any**} [*operator port* [*port*]] {*dest-ip* [*wildcard*] | **host** *dest-ip* | **any**} [*operator port* [*port*]]

where *proto-num* can be 17, which is the equivalent value for UDP.

For ICMP, enter the following command to add a condition:

[**insert** *line-num*] {**deny** | **permit**} {**icmp** | *proto-num*} {*source-ip* [*wildcard*] | **host** *source-ip* | **any**} {*dest-ip* [*wildcard*] | **host** *dest-ip* | **any**} [*icmp-type* [*code*] | *icmp-msg*]

no {**deny** | **permit**} {**icmp** | *proto-num*} {*source-ip* [*wildcard*] | **host** *source-ip* | **any**} {*dest-ip* [*wildcard*] | **host** *dest-ip* | **any**} [*icmp-type* [*code*] | *icmp-msg*]

where *proto-num* can be 2, which is the equivalent value for ICMP.

For extended IP ACLs, the **wildcard** keyword is required if the **host** keyword is not specified. For a list of the keywords that you can use to match specific ICMP message types and codes, see Table 2-11. For a list of supported UDP and TCP keywords, see Table 2-9 and Table 2-10.

Use access lists to control access to specific applications or interfaces on an SE. An access control list consists of one or more condition entries that specify the kind of packets that the SE will drop or accept for further processing. The SE applies each entry in the order in which it occurs in the access list, which by default, is the order in which you configured the entry.

The following are some examples of how IP ACLs can be used in environments that have SEs:

- An SE resides on the customer premises and is managed by a service provider, and the service provider wants to secure the device for its management only.
- An SE is deployed anywhere within the enterprise. As with routers and switches, the administrator wants to limit Telnet, SSH, and SE GUI access to the IT source subnets.
- An application layer proxy firewall with a hardened outside interface has no ports exposed. (*Hardened* means that the interface carefully restricts which ports are available for access, primarily for security reasons. With an outside interface, many types of security attacks are possible.) The SE's outside address is Internet global, and its inside address is private. The inside interface has an IP ACL to limit Telnet, SSH, and SE GUI access to the SE.
- An SE is deployed as a reverse proxy in an untrusted environment. The SE administrator wishes to allow only port 80 inbound traffic on the outside interface and outbound connections on the back-end interface.

Within ACL configuration mode, you can use the editing commands (**list**, **delete**, and **move**) to display the current condition entries, to delete a specific entry, or to change the order in which the entries are evaluated. To return to global configuration mode, enter **exit** at the ACL configuration mode prompt.

To create an entry, use a **deny** or **permit** keyword and specify the type of packets that you want the SE to drop or to accept for further processing. By default, an access list denies everything because the list is terminated by an implicit **deny any** entry. You must include at least one **permit** entry to create a valid access list.

After creating an access list, you can include the access list in an access group using the **access-group** command, which determines how the access list is applied. You can also apply the access list to a specific application using the appropriate command. A reference to an access list that does not exist is the equivalent of a **permit any** condition statement.

To work with access lists, enter either the **ip access-list standard** or **ip access-list extended** global configuration command. Identify the new or existing access list with a name up to 30 characters long beginning with a letter or with a number. If you use a number to identify a standard access list, it must be between 1 and 99; for an extended access list, use a number from 100 to 199. You must use a standard access list for providing access to the SNMP server or to the TFTP gateway/server.

After you identify the access list, the CLI enters the appropriate configuration mode and all subsequent commands apply to the specified access list.

ip access-list standard Command

You typically use a standard access list to allow connections from a host with a specific IP address or from hosts on a specific network. To allow connections from a specific host, use the **permit host** *source-ip* option and replace *source-ip* with the IP address of the specific host.

To allow connections from a specific network, use the **permit** *source-ip wildcard* option. Replace *source-ip* with a network ID or the IP address of any host on the network that you want to specify. Replace *wildcard* with the dotted decimal notation for a mask that is the reverse of a subnet mask, where a 0 indicates a position that must be matched and a 1 indicates a position that does not matter. For instance, the wildcard 0.0.0.255 causes the last eight bits in the source IP address to be ignored. Therefore, the **permit 192.168.1.0 0.0.0.255** entry allows access from any host on the 192.168.1.0 network.

ip access-list extended Command

Use an extended access list to control connections based on the destination IP address or based on the protocol type. You can combine these conditions with information about the source IP address to create more restrictive conditions. Table 2-9 lists the UDP keywords that you can use with extended access lists.

Table 2-9 UDP Keywords and Port Numbers

CLI Keyword	Description	UDP Port Number
bootpc	Bootstrap Protocol (BOOTP) client service	68
bootps	Bootstrap Protocol (BOOTP) server service	67
domain	Domain Name System (DNS) service	53
netbios-dgm	NetBIOS datagram service	138
netbios-ns	NetBIOS name resolution service	137
netbios-ss	NetBIOS session service	139
nfs	Network File System service	2049
ntp	Network Time Protocol settings	123
snmp	Simple Network Management Protocol service	161
snmptrap	SNMP traps	162
tftp	Trivial File Transfer Protocol service	69

Table 2-10 lists the TCP keywords that you can use with extended access lists.

Table 2-10 TCP Keywords and Port Numbers

CLI Keyword	Description	TCP Port Number
domain	Domain Name System	53
exec	Remote process execution	512
ftp	File Transfer Protocol service	21
ftp-data	FTP data connections (used infrequently)	20

Table 2-10 TCP Keywords and Port Numbers (continued)

CLI Keyword	Description	TCP Port Number
nfs	Network File System service applications	2049
rtsp	Real-Time Streaming Protocol applications	554
ssh	Secure Shell login	22
telnet	Remote login using telnet	23
www	World Wide Web (HTTP) service	80

Table 2-11 lists the keywords that you can use to match specific ICMP message types and codes.

Table 2-11 Keywords for ICMP Message Type and Code

Field	Description
administratively-prohibited	Messages that are administratively prohibited from being allowed access.
alternate-address	Messages that specify alternate IP addresses.
conversion-error	Messages that denote a datagram conversion error.
dod-host-prohibited	Messages that signify a Department of Defense (DoD) protocol Internet host denial.
dod-net-prohibited	Messages that specify a DoD protocol network denial.
echo	Messages that are used to send echo packets to test basic network connectivity.
echo-reply	Messages that are used to send echo reply packets.
general-parameter-problem	Messages that report general parameter problems.
host-isolated	Messages that indicate that the host is isolated.
host-precedence-unreachable	Messages that have been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 3 (Host Unreachable). This is the most common response. Large numbers of this datagram type on the network are indicative of network difficulties or may be indicative of hostile actions.
host-redirect	Messages that specify redirection to a host.
host-tos-redirect	Messages that specify redirection to a host for type of service-based (ToS) routing.
host-tos-unreachable	Messages that denote that the host is unreachable for ToS-based routing.
host-unknown	Messages that specify that the host or source is unknown.
host-unreachable	Messages that specify that the host is unreachable.
information-reply	Messages that contain domain name replies.
information-request	Messages that contain domain name requests.
mask-reply	Messages that contain subnet mask replies.
mask-request	Messages that contain subnet mask requests.
mobile-redirect	Messages that specify redirection to a mobile host.

Table 2-11 Keywords for ICMP Message Type and Code (continued)

Field	Description
net-redirect	Messages that are used for redirection to a different network.
net-tos-redirect	Messages that are used for redirection to a different network for ToS-based routing.
net-tos-unreachable	Messages that specify that the network is unreachable for the ToS-based routing.
net-unreachable	Messages that specify that the network is unreachable.
network-unknown	Messages that denote that the network is unknown.
no-room-for-option	Messages that specify the requirement of a parameter, but that no room is unavailable for it.
option-missing	Messages that specify the requirement of a parameter, but that parameter is not available.
packet-too-big	Messages that specify that the ICMP packet requires fragmentation but the Do Not Fragment (DF) bit is set.
parameter-problem	Messages that signify parameter-related problems.
port-unreachable	Messages that specify that the port is unreachable.
precedence-unreachable	Messages that specify that host precedence is not available.
protocol-unreachable	Messages that specify that the protocol is unreachable.
reassembly-timeout	Messages that specify a timeout during reassembling of packets.
redirect	Messages that have been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 5 (Redirect). ICMP redirect messages are used by routers to notify the hosts on the data link that a better route is available for a particular destination.
router-advertisement	Messages that contain ICMP router discovery messages called router advertisements.
router-solicitation	Messages that are multicast to ask for immediate updates on neighboring router interface states.
source-quench	Messages that have been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 4 (Source Quench). This datagram may be used in network management to provide congestion control. A source quench packet will be issued when a router is beginning to lose packets due to the transmission rate of a source. The source quench is a request to the source to reduce the rate of a datagram transmission.
source-route-failed	Messages that specify the failure of a source route.
time-exceeded	Messages that specify information about all instances when specified times were exceeded.
timestamp-reply	Messages that contain time-stamp replies.
timestamp-request	Messages that contain time-stamp requests.
traceroute	Messages that specify the entire route to a network host from the source.

Table 2-11 Keywords for ICMP Message Type and Code (continued)

Field	Description
ttl-exceeded	Messages that specify that ICMP packets have exceeded the Time-To-Live configuration.
unreachable	Messages that are sent when packets are denied by an access list; these packets are not dropped in the hardware but generate the ICMP-unreachable message.

Examples

The following example shows how to create an access list to allow all web traffic and to only allow a specific host administrative access using Secure Shell (SSH):

```
ServiceEngine(config)#ip access-list extended example
ServiceEngine(config-ext-nacl)#permit tcp any any eq www
ServiceEngine(config-ext-nacl)#permit tcp host 10.1.1.5 any eq ssh
ServiceEngine(config-ext-nacl)#exit
```

The following example shows how to activate the access list for an interface:

```
ServiceEngine(config)#interface gigabitethernet 1/0
ServiceEngine(config-if)#exit
```

The following example shows how this configuration appears when you enter the **show running-configuration** command:

```
...
!
ip access-list extended example
 permit tcp any any eq www
 permit tcp host 10.1.1.5 any eq ssh
 exit
. . .
```

Related Commands

clear ip access-list counters
show ip access-list

ipv6

To specify the default gateway's IPv6 address, use the **ipv6** global configuration command. To disable the IPv6 address, use the **no** form of this command.

ipv6 default-gateway *ip-address*

no ipv6 default-gateway *ip-address*

Syntax Description

default-gateway	Specifies the default gateway's IPv6 address.
ip-address	IPv6 address of the default gateway.

Defaults

No default behavior or values.

Command Modes

Global configuration

Examples

The following example shows how to configure an IPv6-related address:

```
ServiceEgine(config)#ipv6 default-gateway fec0::100/64
```

Related Commands

show ipv6
traceroute6

kernel kdb

To enable access to the kernel debugger (kdb), use the **kernel kdb** global configuration command. To disable the kernel debugger, use the **no** form of this command.

kernel kdb

no kernel kdb

Syntax Description

This command has no arguments or keywords.

Defaults

kdb is disabled by default.

Command Modes

Global configuration

Usage Guidelines

Once enabled, kdb is automatically activated when kernel problems occur. Once activated, all normal functioning of the CDS device is suspended until kdb is manually deactivated. The kdb prompt looks like this prompt:

```
[0]kdb>
```

To deactivate kdb, enter **go** at the kdb prompt. If kdb was automatically activated because of kernel problems, you must reboot to recover from the issue. If you activated kdb manually for diagnostic purposes, the system resumes normal functioning in whatever state it was when you activated kdb. In either case, if you enter **reboot**, the system restarts and normal operation resumes.

With the Internet Streamer CDS software earlier than Release 2.4, kdb is enabled by default and cannot be disabled. In the Release 2.0.3 and later releases, kdb is disabled by default and you must enter the kernel kdb command in global configuration mode to enable it. If kdb has been previously enabled, you can enter the **no kernel kdb** global configuration command to disable it.

When kdb is enabled, you can activate it manually from the local console. With Internet Streamer CDS Release 2.4, you can activate it by pressing **Esc-KDB** (press Escape and then press KDB in capitalization).

Examples

The following example shows how to enable kdb:

```
ServiceEngine(config)#kernel kdb
```

The following example shows how to disable kdb:

```
ServiceEngine(config)#no kernel kdb
```

line

To specify terminal line settings, use the **line** global configuration command. To disable terminal line settings, use the **no** form of this command.

line console carrier-detect

no line console carrier-detect

Syntax Description

console	Configures the console terminal line settings.
carrier-detect	Sets the device to check the carrier detect signal before writing to the console.

Defaults

This feature is disabled by default.

Command Modes

Global configuration

Usage Guidelines

You should enable carrier detection if you connect the SE, SR, or CDSM to a modem for receiving calls. If you are using a null-modem cable with no carrier detect pin, the device might appear unresponsive on the console until the carrier detect signal is asserted. To recover from a misconfiguration, you should reboot the device and set the 0x2000 bootflag to ignore the Carrier Detect (CD) setting.

Examples

The following example shows how to specify terminal line settings:

```
ServiceEngine(config)#line console carrier-detect
```