VDS-OS Software Commands

This chapter contains an alphabetical listing of all the commands in VDS-OS software. The VDS-OS 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 (config) mode—For setting, viewing, and testing the configuration of VDS-OS software features for the entire device. To use this mode, enter the **configure** command from privileged EXEC mode.
- Interface configuration (config-if) 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—Several 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 the "Using Command Modes" section on page 1-2 for a complete discussion of using CLI command modes.

Table 2-1 summarizes the VDS-OS commands and indicates the command mode for each command. 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 VDS-OS software device mode determines whether the VDS-OS device is functioning as a Service Engine (SE), Virtual Origin System Manager (VOSM), or Service Router (SR). The commands available from a specific CLI mode are determined by the VDS-OS 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.

Table 2-1 CLI Commands

Command	Description	CLI Mode	Device Mode
access-lists	Configures the access control list entries.	Global configuration	SE
alarm	Configures alarms.	Global configuration	SE, SR

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
asset	Configures the CISCO-ENTITY-ASSET-MIB.	Global configuration	All
banner	Configures the EXEC, login, and message-of-the-day (MOTD) banners.	Global configuration	All
blink	Identifies physical devices by blinking their LED(s).	Privileged-level EXEC	All
cache	Specifies the cache commands. **Note** The **cache** command is not supported in VDS-OS 2.0.	Global configuration	SE
capture-controller	Enables/disables debugging for specific capture-controller modules.	Privileged-level EXEC	SE
cd	Changes the directory.	User-level EXEC and privileged-level EXEC	All
cdn-select	Configures Content Delivery Network-select CDN-select.	Global configuration	SR
cdn-select	Manages the Internet Streamer CDS network file system (CDNFS).	Privileged-level EXEC	SE
clear ip	Clears the IP configuration.	Privileged-level EXEC	All
clear ipv6	Clears the IPv6 configuration.	Privileged-level EXEC	All
clear logging	Clears the syslog messages saved in the disk file.	Privileged-level EXEC	All
clear service-router	Clears the Service Router.	Privileged-level EXEC	SR
clear ssh-key	Clears the Secure Shell (SSH) key for a remote host.	Privileged-level EXEC	SE
clear statistics	Clears the statistics.	Privileged-level EXEC	All
clear transaction-log	Clears and archives the working transaction logs.	Privileged-level EXEC	SE, SR
clear users	Clears the connections (login) of authenticated users.	Privileged-level EXEC	All
clock (EXEC configuration)	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 configuration)	Configures the database parameters that are embedded in the Centralized Management System (CMS).	Privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
cms (global configuration)	Schedules the maintenance and enables the Centralized Management System on a given node.	Global configuration	All
configure	Enters configuration mode from privileged EXEC mode (commands used to access configuration modes).	Privileged-level EXEC	All
content-origin	Supports multiple origin services within a content origin.	Global configuration	SE
copy	Copies the configuration or image files to and from the CD-ROM, flash memory, disk, or remote hosts.	Privileged-level EXEC	All
core-dump	Configures a coredump file.	Privileged-level EXEC	All
cpfile	Copies a file.	User-level EXEC and privileged-level EXEC	All
debug	Configures the debugging options.	Privileged-level EXEC	All
delfile	Deletes a file.	User-level EXEC and privileged-level EXEC	All
deltree	Deletes a directory and its subdirectories.	User-level EXEC and privileged-level EXEC	All
device	Configures the mode of operation on a device.	Global configuration	All
dir	Displays the list of files in a directory.	User-level EXEC and privileged-level EXEC	All
disable	Turns off the privileged EXEC commands.	Privileged-level EXEC	All
disk (EXEC configuration)	Allocates the disks among the CDS network file system (CDNFS) and system file system (sysfs).	Privileged-level EXEC	All
disk (global configuration)	Configures how the disk errors should be handled.	Global configuration	All
dnslookup	Resolves a host or domain name to an IP address.	User-level EXEC and privileged-level EXEC	All
enable (EXEC configuration)	Accesses the privileged EXEC commands.	User-level EXEC and privileged-level EXEC	All
enable (global configuration)	Changes the enable password.	Global configuration	All
end	Exits configuration and privileged EXEC modes.	Global configuration	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
exec-timeout	Configures the length of time that an inactive Telnet or SSH session remains open.	Global configuration	All
exit	Exits from interface, global configuration, or privileged EXEC modes.	All	All
expert-mode	Configures debugshell.	Global configuration	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
ftp	Enables File Transfer Protocol (FTP) services.	Global configuration	All
gulp	Captures lossless gigabit packets and writes them to disk.	Privileged-level EXEC	All
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 HTTP-related parameters	Privileged-level EXEC	SR
install	Installs a new version of the caching application.	Privileged-level EXEC	All
interface	Configures a Gigabit Ethernet or port channel interface. Provides access to interface configuration mode.	Global configuration	All
iostat	Shows CPU and I/O statistics for devices and partitions.	Global configuration	All
ip (global configuration)	Configures the Internet Protocol.	Global configuration	All
ip (interface configuration)	Configures the interface Internet Protocol.	Interface configuration	All
ip access-list	Creates and modifies the access lists for controlling access to interfaces or applications. Provides access to ACL configuration mode.	Global configuration	All
ipv6	Specifies the default gateway's IPv6 address.	Global configuration	All
kernel	Configures the kernel.	Global configuration	All
line	Specifies the terminal line settings.	Global configuration	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
lls	Displays the files in a long-list format.	User-level EXEC and privileged-level EXEC	All
logging	Configures syslog.	Global configuration	All
ls	Lists the files and subdirectories in a directory.	User-level EXEC and privileged-level EXEC	All
mkdir	Makes a directory.	User-level EXEC and privileged-level EXEC	All
mkfile	Makes a file (for testing).	User-level EXEC and privileged-level EXEC	All
model	Changes the CDE250 platform model number after a remanufacturing or rescue process.	User-level EXEC and privileged-level EXEC	All
mount-option	Configures the mount option profile for remote storage.	Global configuration	SE
mpstat	Displays processor-related statistics.	Privileged-level EXEC	SR
netmon	Displays the transmit and receive activity on an interface.	Privileged-level EXEC	All
netstatr	Displays the rate of change of netstat statistics.	Privileged-level EXEC	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 Network Time Protocol (NTP) software clock.	Privileged-level EXEC	All
ping	Sends the echo packets.	User-level EXEC and privileged-level EXEC	All
ping6	Pings the IPv6 address.	User-level EXEC and privileged-level EXEC	All
port-channel	Configures the port channel load balancing options.	Global configuration	All
primary-interface	Configures a primary interface for the VDS-OS network to be a Gigabit Ethernet or port channel interface.	Global configuration	All
pwd	Displays the present working directory.	User-level EXEC and privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
radius-server	Configures the Remote Authentication Dial-In User Service (RADIUS) authentication.	Global configuration	All
reload	Halts a device and performs a cold restart.	Privileged-level EXEC	All
rename	Renames a file.	User-level EXEC and privileged-level EXEC	All
restore	Restores a device to its manufactured default status.	Privileged-level EXEC	All
rmdir	Removes a directory.	User-level EXEC and privileged-level EXEC	All
script	Checks the errors in a script or executes a script.	Privileged-level EXEC	All
service	Specifies the type of service.	Privileged-level EXEC	All
service-router	Configures service routing.	Global configuration	All
setup	Configures the basic configuration settings and a set of commonly used caching services.	Privileged-level EXEC	All
show access-lists	Displays the access control list configuration.	User-level EXEC and privileged-level EXEC	SE
show alarms	Displays information on various types of alarms, their status, and history.	User-level EXEC and privileged-level EXEC	All
show arp	Displays the Address Resolution Protocol entries.	User-level EXEC and privileged-level EXEC	All
show authentication	Displays the authentication configuration.	User-level EXEC and privileged-level EXEC	All
show banner	Displays information on various types of banners.	User-level EXEC and privileged-level EXEC	All
show cdnfs	Displays the VDS-OS network file system information.	User-level EXEC and privileged-level EXEC	SE
show clock	Displays the system clock.	User-level EXEC and privileged-level EXEC	All
show cms	Displays the Centralized Management System protocol, embedded database content, maintenance status, and other information.	User-level EXEC and privileged-level EXEC	All
show content	Displays all content entries in the VDS-OS.	User-level EXEC and privileged-level EXEC	SE

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
show content-origin	Displays information about the Network-Attached Storage (NAS) mount.	User-level EXEC and privileged-level EXEC	SE
show debugging	Displays the state of each debugging option.	User-level EXEC and privileged-level EXEC	All
show device-mode	Displays the configured or current mode of a VOSM, SE, or SR device.	User-level EXEC and privileged-level EXEC	All
show disks	Displays the disk configurations.	User-level EXEC and privileged-level EXEC	All
show flash	Displays the flash memory information.	User-level EXEC and privileged-level EXEC	All
show ftp	Displays the caching configuration of the FTP.	User-level EXEC and privileged-level EXEC	All
show hardware	Displays the system hardware information.	User-level EXEC and privileged-level EXEC	All
show hosts	Displays the IP domain name, name servers, IP addresses, and host table.	User-level EXEC and privileged-level EXEC	All
show interface	Displays the hardware interface information.	User-level EXEC and privileged-level EXEC	All
show inventory	Displays the system inventory information.	User-level EXEC and privileged-level EXEC	All
show ip	Displays the contents of a particular host in the Border Gateway Protocol (BGP) routing table.	User-level EXEC and privileged-level EXEC	All
show ipv6	Displays IPv6 information.	User-level EXEC and privileged-level EXEC	All
show lacp	Displays LACP information.	User-level EXEC and privileged-level EXEC	All
show logging	Displays the system logging configuration.	User-level EXEC and privileged-level EXEC	All
show mount-option	Displays mount options.	User-level EXEC and privileged-level EXEC	SE
show ntp	Displays the Network Time Protocol configuration status.	User-level EXEC and privileged-level EXEC	All
show processes	Displays the process status.	User-level EXEC and privileged-level EXEC	All
show radius-server	Displays the RADIUS server information.	User-level EXEC and privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
show running-config	Displays the current operating configuration.	User-level EXEC and privileged-level EXEC	All
show service-router	Displays the Service Router configuration.	User-level EXEC and privileged-level EXEC	All
show services	Displays the services-related information.	User-level EXEC and privileged-level EXEC	All
show snmp	Displays the Simple Network Management Protocol (SNMP) parameters.	User-level EXEC and privileged-level EXEC	All
show ssh	Displays the Secure Shell status and configuration.	User-level EXEC and privileged-level EXEC	All
show standby	Displays the information related to the standby interface.	User-level EXEC and privileged-level EXEC	All
show startup-config	Displays the startup configuration.	User-level EXEC and privileged-level EXEC	All
show statistics access-lists	Displays the access control list statistics.	User-level EXEC and privileged-level EXEC	SE
show statistics admission	Displays admission control statistics.	User-level EXEC and privileged-level EXEC	SE
show statistics cdnfs	Displays the SE VDS-OS network file system statistics.	User-level EXEC and privileged-level EXEC	SE
show statistics content-mgr	Displays the Content Manager statistics.	User-level EXEC and privileged-level EXEC	SE
show statistics fd	Displays the file descriptors limits.	User-level EXEC and privileged-level EXEC	All
show statistics icmp	Displays the Internet Control Message Protocol (ICMP) statistics.	User-level EXEC and privileged-level EXEC	All
show statistics icmpv6	Displays the ICMPv6 statistics.	User-level EXEC and privileged-level EXEC	All
show statistics ip	Displays the Internet Protocol statistics.	User-level EXEC and privileged-level EXEC	All
show statistics lsof	Displays the List of Open File descriptors.	User-level EXEC and privileged-level EXEC	All
show statistics netstat	Displays the Internet socket connection statistics.	User-level EXEC and privileged-level EXEC	All
show statistics radius	Displays the RADIUS authentication statistics.	User-level EXEC and privileged-level EXEC	All
show statistics service-router	Displays the Service Router statistics.	User-level EXEC and privileged-level EXEC	SR

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
show statistics services	Displays the services statistics.	User-level EXEC and privileged-level EXEC	SR, VOSM
show statistics snmp	Displays the SNMP statistics.	User-level EXEC and privileged-level EXEC	All
show statistics tacacs	Displays the Service Engine (SE) Terminal Access Controller Access Control System Plus (TACACS+) authentication and authorization statistics.	User-level EXEC and privileged-level EXEC	All
show statistics tcp	Displays the Transmission Control Protocol (TCP) statistics.	User-level EXEC and privileged-level EXEC	All
show statistics transaction-logs	Displays the transaction log export statistics.	User-level EXEC and privileged-level EXEC	SE, SR
show statistics udp	Displays the User Datagram Protocol (UDP) statistics.	User-level EXEC and privileged-level EXEC	All
show statistics vos	Displays VDS-OS statistics.	User-level EXEC and privileged-level EXEC	SE
show statistics web-engine	Displays the Web Engine statistics.	User-level EXEC and privileged-level EXEC	SE
show tacacs	Displays TACACS+ authentication protocol configuration information.	User-level EXEC and privileged-level EXEC	All
show tech-support	Displays the system information for Cisco technical support.	User-level EXEC and privileged-level EXEC	All
show telnet	Displays the Telnet services configuration.	User-level EXEC and privileged-level EXEC	All
show transaction-logging	Displays the transaction logging information.	User-level EXEC and privileged-level EXEC	SE, SR
show url-signature	Displays the URL signature information.	User-level EXEC and privileged-level EXEC	SE
show user	Displays the user identification number and username information.	User-level EXEC and privileged-level EXEC	All
show users	Displays the specified users.	User-level EXEC and privileged-level EXEC	All
show version	Displays the software version.	User-level EXEC and privileged-level EXEC	All
show vos	Displays VDS-OS information.	User-level EXEC and privileged-level EXEC	SE
show web-engine	Displays the Web Engine information.	User-level EXEC and privileged-level EXEC	SE
shutdown (interface configuration)	Shuts down the specified interface.	Interface configuration	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
shutdown (EXEC configuration)	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 Management Information Base (MIB) object sysContact.	Global configuration	All
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 an SNMPv2 MIB view.	Global configuration	All
ss	Dumps socket statistics.	Privileged-level EXEC	All
ssh-key-generate	Generates the SSH host key.	Global configuration	All
sshd	Configures the SSH service parameters.	Global configuration	All
streaming-interface	Configures the streaming interface.	Global configuration	SE
sysreport	Saves the sysreport to 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
tcpdumpx	Dumps the network traffic with the tcpdump extension for a multi-interface capture.	Privileged-level EXEC	All
tcpmon	Searches all TCP connections.	Privileged-level EXEC	All
tcp	Configures TCP-related parameters.	Global configuration	All
telnet (EXEC configuration)	Starts the Telnet client.	User-level EXEC and privileged-level EXEC	All
telnet (global configuration)	Enables Telnet service.	Global configuration	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
terminal	Sets the terminal output commands.	User-level EXEC and privileged-level EXEC	All
test-url	Tests the accessibility of a URL using FTP, HTTP, or HTTPS.	User-level EXEC and privileged-level EXEC	SE, SR
top	Displays a dynamic real-time view of a running VDS-OS.	Privileged-level EXEC	All
traceroute	Traces the route to a remote host.	User-level EXEC and privileged-level EXEC	All
traceroute6	Traces the route to a remote IPv6-enabled host.	User-level EXEC and privileged-level EXEC	All
transaction-log force	Forces archiving of the working log file to make a transaction log file.	Privileged-level EXEC	SE, SR
transaction-logs	Configures and enables the transaction logging parameters.	Global configuration	SE, SR
type	Displays a file.	User-level EXEC and privileged-level EXEC	All
type-tail	Displays the last several lines of a file.	User-level EXEC and privileged-level EXEC	All
undebug	Disables debugging functions.	Privileged-level EXEC	All
url-signature	Configures the URL signature.	Global configuration	SE
username	Establishes the username authentication.	Global configuration	All
vosm	Configure the VDS-OS IP address to be used for the SEs or SRs, or configures the role and GUI parameters on a Virtual Origin Server Manager (VOSM) device.	Global configuration	All
web-engine (EXEC configuration)	Configures the Web Engine.	User-level EXEC	SE
web-engine (global configuration)	Configures the Web Engine caching parameters and disables revalidation. **Note** The **web-engine revalidation** command is not supported in VDS-OS 2.0.	Global configuration	SE

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
whoami	Displays the current user's name.	User-level EXEC and privileged-level EXEC	All
write	Writes or erases the startup configurations to nonvolatile random-access memory (NVRAM) or to a terminal session, or writes the MIB persistence configuration to disk.	Privileged-level EXEC	All

access-lists

To configure access control list (ACL) entries, use the **access-lists** command in global configuration mode. 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 ACL record within the access list.
number	(Optional) Position number within the ACL. The range is from 1 to 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 ACL.

Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

You can configure group authorization using an ACL only after a user has been authenticated against a Lightweight Directory Access Protocol (LDAP) HTTP-request Authentication Server. The use of this list configures group privileges when members of the group are accessing content provided by an 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 an SE. For instance, use the **access-lists 300 deny groupname marketing** command to prevent any user from the marketing group from accessing content through an 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.

The ACL 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 strin*g is a case-sensitive string with mixed-case alphanumeric characters.
- 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.

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

For Windows-based user groups, 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.

Wildcards

The **access-list** command does not use a netmask; it uses a wildcard bitmask. The source and destination IP and wildcard usage is as follows:

- **source_ip**—Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source:
  - Use a 32-bit quantity in four-part dotted decimal format.
  - Use the **any** keyword => source and source-wildcard of 0.0.0.0 255.255.255.255.
  - Use the **host** keyword => specific source and source_wildcard equal 0.0.0.0.
- **source-wildcard**—Wildcard bits to be applied to source. Each wildcard bit set to 0 indicates the corresponding bit position in the source. Each wildcard bit set to 1 indicates that both a 0 bit and a 1 bit in the corresponding position of the IP address of the packet is considered a match to this access list entry.

  To specify the source wildcard, use a 32-bit quantity in four-part dotted decimal format. Place 1s in the bit positions you want to ignore.

Note Wildcard bits set to 1 need not be contiguous in the source wildcard. For example, a source wildcard of 0.255.0.64 would be valid.

Examples

The following example shows how to display the configuration of the ACL 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 ACL 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 ACL 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

Command	Description
show access-lists 300	Displays the ACL configuration.
show statistics access-list 300	Displays the ACL statistics.

alarm

To configure alarms, use the **alarm** command in global configuration mode. To disable alarms, use the **no** form of this command.

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

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

Syntax Description

admin-shutdown-alarm	Generates a linkdown alarm when an interface shuts down.
enable	Enables admin shutdown alarm overload detection.
overload-detect	Specifies alarm overload configuration.
clear	Specifies the threshold below which the alarm overload state on an SE is cleared and the Simple Network Management Protocol (SNMP) traps and alarm notifications to the Centralized Management System (CMS) resume. **Note** The **alarm overload-detect clear** command 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 content delivery engine (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	Enables the detection of alarm overload situations.

Defaults

admin-shutdown-alarm: disabled

raise: 10 alarms per second

clear: 1 alarm per second

Command Modes

Global configuration (config) mode.

Usage Guidelines

The **alarm admin-shutdown-alarm** command must be enabled for an admin-shutdown alarm to take effect. If an admin-shutdown alarm occurs, disabling this option does not clear the outstanding alarm properly. There are two ways to avoid this situation:

- Clear the outstanding admin-shutdown alarm first before disabling this option.
- Disable this option and reboot, which clears this alarm.

When multiple applications running on an SE experience problems at the same time, numerous alarms are set off simultaneously, and an SE may stop responding. Use the **alarm overload-detect** 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, an SE enters an alarm overload state until the number of alarms drops down to the number defined in the **clear**.

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

- 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.
- Alarm overload clear notification is sent.
- 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 an SE. The **show alarms** and **show alarms history** command in EXEC configuration modes display all the alarms even in the alarm overload state.

Examples

The following example shows how to generate a linkdown alarm when an interface shuts down:

```
ServiceEngine(config)# alarm admin-shutdown-alarm enable
```

The following example shows how to enable the detection of alarm overload:

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

The following example shows how to set the threshold for triggering the alarm overload at 100 alarms per second:

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

The following example shows how to set the level for clearing the alarm overload at 10 alarms per second:

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

Related Commands

Command	Description
show alarms	Displays information on various types of alarms, their status, and history.
show alarm status	Displays the status of various alarms and alarm overload settings.

asset

To configure the CISCO-ENTITY-ASSET-MIB, use the **asset** command in global configuration mode. 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

None

Command Modes

Global configuration (config) mode.

Examples

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

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

banner

To configure the EXEC, login, and message-of-the-day (MOTD) banners, use the **banner** command in global configuration mode. 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 (config) mode.

Usage Guidelines

You can configure the following three types of banners in any VDS-OS software device mode:

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

Note All 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** command to enable banner support on the SE. Enter the **show banner** command in EXEC configuration mode 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** 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 a VDS-OS 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 a VDS-OS 2.3 device\n"
```

The following example shows how to use the **banner login message** 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** 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 VDS-OS username and password to log in to this SE.\n
.
Message has 99 characters.
ServiceEngine(config)#
```

Assume that the 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 sees 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 a VDS-OS 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 VDS-OS 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 VDS-OS username and password to log in to this SE.
```

After the user enters a valid VDS-OS 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 configuration mode CLI prompt is displayed:

```
ServiceEngine#
```

Related Commands

Command	Description
show banner	Enables banner support on the SE.

blink

To identify physical devices by blinking their LED(s), use the **blink** command in EXEC configuration mode.

blink {**disk** *name* | **interface {GigabitEthernet** *slot/port_num* | **TenGigabitEthernet** *slot/port_num*}}

Syntax Description

disk	Flash disk LED for 3s.
name	disk name (format is disk00).
interface	Flash network interface port LED for 3s.
GigabitEthernet	Selects a Gigabit Ethernet interface.
slot/port_num	Slot and port number for the selected interface. The slot range is from 1 to 14; the port range is from 0 to 0. The slot number and port number are separated with a forward slash character (/).
TenGigabitEthernet	Selects a Ten Gigabit Ethernet interface.

Command Default

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **blink disk** command submits IO to a disk, do not use this command in systems with live traffic.

Examples

The following example shows how to blink a disk:

```
ServiceRouter# blink disk disk00
Blinking disk00 LED for 3 seconds
```

The following example shows how to blink a GigabitEthernet interface:

```
ServiceRouter# blink interface gigabitEthernet 1/0
Blinking eth0 LED for 3 seconds
```

cache

To restrict the maximum number of contents in the VDS-OS, use the **cache** command in global configuration mode.

cache content {**eviction-preferred-size** {**small** | **large**} | **eviction-protection** {**min-size-100MB** {**min-duration-1hr** | **min-duration-2hr** | **min-duration-3hr** | **min-duration-4hr**}| **min-size-1GB** {**min-duration-1hr** | **min-duration-2hr** | **min-duration-3hr** | **min-duration-4hr**} | **min-size-4GB** {**min-duration-1hr** | **min-duration-2hr** | **min-duration-3hr** | **min-duration-4hr**} | **min-size-500MB** {**min-duration-1hr** | **min-duration-2hr** | **min-duration-3hr** | **min-duration-4hr**}}| **max-cached-entries** *num*

Syntax Description

content	Configures the cached contents.
eviction-preferred-size	Configures cache content eviction preferred.
large	Selects cache content eviction preferred size (Retain smaller objects).
small	Selects cache content eviction preferred size (Retain larger objects).
eviction-protection	Configures the eviction protection.
min-size-100MB	Minimum cache entry size to protect.
min-duration-1hr	Minimum duration to protect the content from eviction.
min-duration-2hrs	Minimum duration to protect the content from eviction.
min-duration-3hrs	Minimum duration to protect the content from eviction.
min-duration-4hrs	Minimum duration to protect the content from eviction.
min-size-1GB	Minimum cache entry size to protect.
min-size-4GB	Minimum cache entry size to protect.
min-size-500MB	Minimum cache entry size to protect.
max-cached-entries	Cleans up the unwanted entries in the CDS network file system (CDNFS).
num	Max cached entries. The range is from 1 to 20000000.

Defaults

The max-cached-entries default is 2000000 entries.

Command Modes

Global configuration (config) mode.

Usage Guidelines

The **cache** command is not supported in VDS-OS 2.0.

The Content Manager manages the caching, storage, and deletion of content.

Current priority favors small objects. The **cache content eviction-preferred size** command allows users to configure a preference for small or large objects in the Content Manager. Once a preference is specified, it only applies on contents made after the configurative; contents prior to configuration remain unchanged.

Addition and Deletion Processes

Previously, the VDS-OS software did not restrict adding new content to CDNFS as long as there was enough disk space for the asset. The **cache content max-cached-entries** command restricted the number of assets, but it was not a hard limit. New content was always added and the VDS-OS would delete old content in an attempt to keep within the limits configured. The VDS-OS could actually have more content than the configured limit, because the process to delete content is slower than the process to add content. The same situation applies to disk-usage based deletion, where deletion occurs when 90 percent of the CDNFS is used.

Content addition stops at 105 percent of the maximum object count or 95 percent of the CDNFS capacity (disk usage). For example, if the maximum number of objects has been configured as 20 million (which is the default value), the VDS-OS starts deleting content if the object count reaches 20 million, but adding content is still allowed. Adding content stops when the maximum number of content objects reaches 21 million (105 percent of 20 million), which allows time for the content deletion process to reduce the number of objects in the VDS-OS to the configured limit. Adding content resumes only after the number of objects is 20 million or less. The same logic applies to disk usage. The deletion process starts when disk usage reaches 93 percent, adding content stops when disk usage reaches 98 percent, and adding content resumes only after the disk usage percentage reaches 95 percent or less.

Note We recommend that any content delivery engine (CDE) model that has hard-disk drives (HDDs) (instead of solid-state drives [SDDs]), and is used to stream ABR content, be configured with a maximum of 5 million objects instead of the default of 20 million. This is because HDD-based hardware requires more seek time to access content. The software can handle 20 million objects, but the hard-drive access time impacts the ABR streaming performance. ABR content consists of a large number of small files, which results in a lot of overhead.

If adding content has been stopped because either the content count reached 105 percent of the limit or the disk usage reached 98 percent of capacity, the un-writable flag is set in the share memory and when the protocol engine calls create, FastCAL library looks into the share memory and denies the creation request. The protocol engine performs a bypass or cut-through operation.

The **show cdnfs usage** command shows the current status of whether the content is able to be cached or not. Following is an example of the output:

```
ServiceEngine# show cdnfs usage
Total number of CDNFS entries  :    2522634
Total space                    :     4656.3 GB
Total bytes available          :     4626.0 GB
Total cache size               :        2.4 GB
Total cached entries           :    2522634
Cache-content mgr status       : Cacheable
Units: 1KB = 1024B; 1MB = 1024KB; 1GB = 1024MB
```

If the maximum object count is reached, the following is displayed:

```
Cache-content mgr status: Not cacheable on the following disk(s): [/disk00-06]
[/disk01-06] [/disk02-01]
105% of max obj count reached :        [/disk00-06] [/disk01-06] [/disk02-01]
```

If the disk usage reaches more than 98 percent, the following is displayed:

```
Cache-content mgr status: Not cacheable on the following disk(s): [/disk01-06]
[/disk02-01]
98% of disk usage reached:       [/disk01-06] [/disk02-01]
```

Eviction Protection

The Content Manager provides configurable eviction protection for some content. The Content Manager eviction algorithm is triggered when the disk usage reaches 93 percent or when the cached object count reaches the configured maximum object count. The eviction algorithm assigns a priority number to each content object based on an algorithm similar to the greedy-dual-size-frequency (GDSF) algorithm. The priority number is based on the size and usage of the object. Small objects are given preference over large objects; that is, they are less likely to be deleted.

To protect incoming large objects from getting a low priority and being deleted, use the **cache content eviction-protection global configure** command. The **cache content eviction-protection** command allows you to set the minimum content size (100 MB, 500 MB, 1 GB, and 4 GB) and the minimum age (1-4 hours for 100 MB size, 1, 4, 8, or 24 hours for all other sizes) of the content object to be protected from deletion. For example, to set the eviction protection for content objects larger than 100 MB that were ingested in the last two hours, you would enter the following command:

```
ServiceEngine(config)# cache content eviction-protection min-size-100MB min-duration-2hrs
```

If the content object being cached is larger than the configured size, it is inserted into a protection table along with the current time stamp. If the difference between the object's time stamp and the current time is greater than the configured time duration, the object is removed from the protection table. If the eviction algorithm is triggered, before it selects an object for deletion, it first looks at the protection table, and if the object is found, it is skipped for that iteration. The **clear-cache-content** command also checks the protection table before deleting an object. The **clear-cache-all** command does not check the eviction protection table; cache content is just deleted. As for relative cache content, content in the protection table might still be deleted if the relative content that is not protected is deleted. The eviction protection is disabled by default.

If the Content Manager eviction algorithm is not able to find any content to delete, a syslog message is sent to notify the administrator to revisit the configuration. Changing the settings of the cache content eviction-protection command only affect the content that are currently in the protection table and any new content that is added. Any object that is removed from the protection table prior to the configuration change is not brought back into the protection table.

Reloading the SE or entering the **no cache content eviction-protection min-size-xx duration-xx** command removes all entries in the eviction protection table.

Note Changing the time on the SE affects the Content Manager eviction process. If the time is set forward, content is deleted sooner than expected. If the time is set back, content is protected longer.

The **show content** command displays the eviction protection status and the number of elements in the eviction protection table.

Note The **cache** command is not supported in VDS-OS 2.0.

Examples

The following example shows how to configure the cache content:

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

The **show cdnfs usage** command shows the current status of whether the content is able to be cached or not. Following is an example of the output:

```
# show cdnfs usage
Total number of CDNFS entries  :    2522634
Total space                    :     4656.3 GB
```

```
Total bytes available          :     4626.0 GB
Total cache size               :        2.4 GB
Total cached entries           :    2522634
Cache-content mgr status       : Cacheable
Units: 1KB = 1024B; 1MB = 1024KB; 1GB = 1024MB
```

If the maximum object count is reached, the following is displayed:

```
Cache-content mgr status       : caching paused[ max count 105% of configured reached ]
```

If the disk usage reaches more than 95 percent, the following is displayed:

```
Cache-content mgr status       : caching paused[ disk max 95% of disk usage reached ]
```

Note When the VDS-OS is started or the cache Content Manager is restarted, it performs a scan of the entire CDNFS. During this period, the deletion starts at 94 percent (not 90 percent) and adding content stops at 95 percent.

Related Commands

Command	Description
show content	Displays a list of cached contents.

capture-controller

To enables/disables debugging for specific capture-controller modules, use the **capture-controller** command in EXEC configuration mode.

capture-controller {**debug module** {**all** | **app** | **http-client** | **httpsession-mgr** | **none** | **parser** | **scheduler**} **undebug module** {**app** | **http-client** | **httpsession-mgr** | **parser** | **scheduler**}}

Syntax Description

debug module	Debug specific capture-controller modules.
all	Enables debug for all modules.
app	App module.
http-client	HTTP-client module.
httpsession-mgr	HTTPSession-Mgr module.
none	Disables debug for all modules.
parser	Parser module.
scheduler	Scheduler module.
undebug-module	Undebugs specific capture-controller modules.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

When debug capturecontroller trace is turned on, the CLI helps limit the volume of logs to specific modules of interest. It is recommended to keep “app” and “scheduler” modules turned on.

Examples

The following example shows how to disable debugging for all modules:

```
ServiceEngine# capture-controller debug-module none
ServiceEngine#
```

cd

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

cd *directoryname*

Syntax Description

directoryname	Directory name.

Defaults

None

Command Modes

EXEC configuration mode.

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

Command	Description
deltree	Deletes a directory and its subdirectories.
dir	Displays the files in a long list format.
lls	Displays the files in a long list format.
ls	Lists the files and subdirectories in a directory.
mkdir	Makes a directory.
pwd	Displays the present working directory.

cdnfs

To browse the CDS network file system (CDNFS), use the **cdnfs browse** command in EXEC configuration mode.

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	Summary information of the garbage entries. No cleanup.
start	Starts the CDNFS garbage collection.
force	Forces removing objections that are in transient states.
stop	Stops the CDNFS garbage collection.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The CDNFS stores the prepositioned VDS-OS network content to be delivered by all supported protocols.

Use the **cdnfs browse** command to browse the CDNFS directories and files. It does not display cached content for the Web Engine. It only caches content for Windows Media Streaming and displays prefetched content. To display cached content, use the **show cache content** command.

```
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 contains information, it lists the websites as directories, and file attributes and content could be viewed using these subcommands.

The **cdnfs cleanup** command, which is used to cleanup unwanted entries in CDNFS, is deprecated in Release 2.6. in the following manner. When an SE is removed from a delivery service, the Content Manager removes all cache content for that delivery service. All prefetched content for that delivery service is removed by the Acquisition and Distribution process. However, if the Acquisition and Distribution process fails because of an SE being offline or for any other reason, then the **cdnfs cleanup** command is still required to remove the prefetched content.

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** command can be used to clean up all UNS content associated with deleted channels.

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

The **cdnfs database recover** command must be run when the cdnfs_db_corrupt alarm is raised. This alarm is raised when the Total Cached entries is more than Total CDNFS entries in the output for the **show cdnfs usage** command:

```
ServiceEngine# show cdnfs usage
Total number of CDNFS entries  :        202
Total space                    :     5037.9 GB
Total bytes available          :     5019.5 GB
Total cache size               :       21.0 GB
Total cached entries           :        218
Cache-content mgr status       : Cacheable
 Units: 1KB = 1024B; 1MB = 1024KB; 1GB = 1024MB
```

This occurs generally when an internal bookkeeping file is corrupted. With the server in the offloading status, enter the **cdnfs database recover** command to remove this inconsistency, then reload the server.

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
```

The following example shows the output for the **cdnfs database recover** command:

```
ServiceEngine# cdnfs database recover
CDNFS database inconsistency issue found.
CDNFS database recovery operation would impact existing and new client sessions.
Recovering database would need device in offloaded state.
```

```
Do you want to recover the CDNFS database now (y/n)?
y
Recovering CDNFS database. It may take few minutes.
Please wait...
CDNFS database recovery is complete. Please reload the device now.
ServiceEngine# reload
Proceed with reload? [confirm] yes
Shutting down all services, will timeout in 15 minutes.
reload in progress...
```

Related Commands

Command	Description
show cdnfs	Displays the CDS network file system information.
show statistics cdnfs	Displays the SE CDS network file system statistics.

cdn-select

To enable the Content Delivery Network (CDN) selector, use the **cdnfs browse** command in EXEC configuration mode.

cdn-select enable

Syntax Description

enable	Enables the CDN selector

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

T

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
```

The following example shows the output for the **cdnfs database recover** command:

```
ServiceEngine# cdnfs database recover
CDNFS database inconsistency issue found.
CDNFS database recovery operation would impact existing and new client sessions.
Recovering database would need device in offloaded state.
Do you want to recover the CDNFS database now (y/n)?
y
Recovering CDNFS database. It may take few minutes.
Please wait...
CDNFS database recovery is complete. Please reload the device now.
ServiceEngine# reload
Proceed with reload? [confirm] yes
Shutting down all services, will timeout in 15 minutes.
reload in progress...
```

Related Commands

Command	Description
show cdnfs	Displays the CDS network file system information.
show statistics cdnfs	Displays the SE CDS network file system statistics.

clear ip

To clear the IP configuration, use the **clear ip** command in EXEC configuration mode.

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

Syntax Description

access-list	Clears the IP access list statistical information.
counters	Clears the IP access list counters.
standard_acl_num	(Optional) Counters for the specified access list, identified using a numeric identifier. The range is from 1 to 99.
extended_acl_num	(Optional) Counters for the specified access list, identified using a numeric identifier. The range is from 100 to 199
acl-name	(Optional) Counters for the specified access list, identified using an alphanumeric identifier up to 30 characters, beginning with a letter.

Command Default

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to clear IP counters:

```
ServiceRouter# clear ip counters
ServiceRouter#
```

Related Commands

Command	Description
show ip bgp summary	Displays the status of all Border Gateway Protocol (BGP) connections.

clear ipv6

To clear the IPv6 ACL counters, use the **clear ipv6** command in EXEC configuration mode.

clear ipv6 access-list counters [*standard_acl-num* | *extended_acl_num* | *acl_name*]

Syntax Description

access-list	Clears the IP access list statistical information.
counters	Clears the IP access list counters.
standard_acl_num	(Optional) Counters for the specified access list, identified using a numeric identifier. The range is from 1 to 99.
extended_acl_num	(Optional) Counters for the specified access list, identified using a numeric identifier. The range is from 100 to 199
acl-name	(Optional) Counters for the specified access list, identified using an alphanumeric identifier up to 30 characters, beginning with a letter.

Defaults

No

Command Modes

EXEC configuration mode.

Examples

The following example shows how to clear IPv6 ACL counters:

```
ServiceRouter# clear ipv6 access-list counters 99
ServiceRouter#
```

Related Commands

Command	Description
ipv6	Specifies the default gateway's IPv6 address.
show ipv6	Displays the IPv6 information.
traceroute6	Traces the route to a remote IPv6-enabled host.

clear logging

To clear the syslog messages saved in the disk file, use the **clear logging** command in EXEC configuration mode.

clear logging

Syntax Description

This command has no keywords or arguments.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

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
```

Examples

The following example shows how to clear the syslogs:

```
ServiceRouter# clear logging
U11-CDE220-2#
```

clear service-router

To clear the Service Router cache, use the **clear service-router** command in EXEC configuration mode.

clear service-router

Syntax Description

This command has no keywords.

Defaults

Clears the cache for all proximity ratings.

Command Modes

EXEC configuration mode.

Usage Guidelines

The **clear service-router** command is used to force clear cache.

Examples

The following example shows how to clear the Service Router.

```
ServiceRouter# clear service-router
ServiceRouter#
```

Related Commands

Command	Description
show service-router	Shows the cache timeout period.

clear ssh-key

To clear the Secure Shell (SSH) key for a remote host, use the **clear ssh-key** command in EXEC configuration mode.

clear ssh-key *line*

Syntax Description

line	Remote host or IP address.

Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to clear the ssh key for a remote host:

```
ServiceEngine# clear ssh-key line
ServiceEngine#
```

Related Commands

Command	Description
ssh-key generate	Generates an ssh key.

clear statistics

To clear the statistics, use the **clear** s**tatistics** command in EXEC configuration mode.

On the SE:

clear statistics {**access-lists 300** | **admission** | **all** | **history** | **icap** | **icmp** | **icmpv6** | **ip** | **radius** | **running** | **snmp** | **tacacs** | **tcp** | **transaction-logs** | **udp** | **vos** | **web-engine** [**force**]}

On the SR:

clear statistics {**all** | **history** | **http requests** | **icmp** | **icmpv6** | **ip** | **radius** | **running** | **service-router** | **snmp** | **tacacs** | **tcp** | **udp**}

On the VOSM:

clear statistics {**all** | **history** | **icmp** | **icmpv6** | **ip** | **radius** | **running** | **snmp** | **tacacs** | **tcp** | **udp**}

Syntax Description

access-lists	Clears the ACL statistics.
300	Clears the group name-based ACL.
admission	Clears admission statistics.
all	Clears all statistics.
history	Clears the statistics history.
http	Clears HTTP statistics.
icap	Clears the Internet Content Adaptation Protocol (ICAP) statistics.
icmp	Clears the Internet Control Message Protocol (ICMP) statistics.
icmpv6	Clears the ICMPv6 statistics.
ip	Clears the IP statistics.
radius	Clears the RADIUS statistics.
running	Clears the running statistics.
service-router	Clears Service Router statistics.
snmp	Clears the Simple Network Management Protocol (SNMP) statistics.
tacacs	Clears the Terminal Access Controller Access Control System Plus (TACACS+) statistics.
tcp	Clears the TCP statistics.
transaction-logs	Clears the transaction log export statistics.
udp	Clears the UDP statistics.
vos	Clears VDS-OS statistics.
web-engine	Clears Web Engine statistics.
force	(Optional) Clears Web Engine detail statistics.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

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 statistics web-engine** and **clear statistics all** commands clear only normal statistics, not the Web Engine statistics details. To clear all Web Engine statistics, use the **clear statistics web-engine force** command.

Note The **clear statistics web-engine** and **clear statistics all** commands clear only normal statistics, not the Web Engine statistics details. To clear all Web Engine statistics, use the **clear statistics web-engine force** command. We do not recommend using the **clear statistics web-engine force** command, but if it is used, restart the Web Engine service by entering the **web-engine stop** and **web-engine start** commands.

Examples

The following example shows how to clear all statistics on the Service Router:

```
ServiceRouter# clear statistics all
ServiceRouter#
```

Related Commands

Command	Description
show statistics	Displays statistics information.

clear transaction-log

To clear and archive the working transaction log files, use the **clear transaction-log** command in EXEC configuration mode.

clear transaction-log

Syntax Description

This command has no keywords or arguments.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

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.

Examples

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

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

Related Commands

Command	Description
show statistics transaction-logs	Displays SE transaction log export statistics.
show transaction-logging	Displays transaction log information.
transaction-log force	Forces the archive or export of the transaction log.
transaction-logs	Configures and enables transaction logs.

clear users

To clear the connections (login) of authenticated users, use the **clear users** command in EXEC configuration mode.

clear users administrative

Syntax Description

administrative	Clears the connections of administrative users who have been authenticated through a remote login service.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

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 how to clear the connections of the authenticated users:

```
ServiceRouter# clear users administrative
ServiceRouter#
```

Related Commands

Command	Description
show user	Displays the user identification number and username information for a particular user.
show users	Displays the specified users.
username	Establishes the username authentication.

clock (EXEC configuration)

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

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 to 23; mm: 00 to 59; ss: 00 to 59).
day	Day of the month. The range is from 1 to 31.
month	Month of the year (January, February, March, April, May, June, July, August, September, October, November, December).
year	Year. The range is from 1993 to 2035.
update-calendar	Updates the calendar with the system clock.

Defaults

None

Command Modes

EXEC configuration mode.

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 have to set the system clock manually. Enter the local time when setting the clock. The SE calculates the Coordinated Universal Time (UTC) based on the time zone set by the **clock timezone** command.

Note We strongly recommend that you configure the SE for the NTP by using the **ntp** command. See the "ntp" section on page 2-158 for more details.

Note If you change the local time on the device, you must change the BIOS clock time as well; otherwise, the timestamps on the error logs are not synchronized. Changing the BIOS clock is required because the kernel does not handle time zones.

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 that 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 NTP clock source, you do not have 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** command.

Examples

The following example shows how to set the software clock on the SE:

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

Related Commands

Command	Description
clock timezone	Sets the clock timezone.
ntp	Configures the Network Time Protocol server.
show clock detail	Displays the UTC and local time.

clock (global configuration)

To set the summer daylight saving time and time zone for display purposes, use the **clock** command in global configuration mode. 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 to start. The range is from 1 to 31.
startmonth	Month to start. The range is from January through December.
startyear	Year to start. The range is from 1993–2032.
starthour	Hour to start in (hh:mm) format. The range is from 0 to 23.
endday	Date to end. The range is from 1 to 31.
endmonth	Month to end. The range is from January through December.
endyear	Year to end. The range is from 1993–2032.
endhour	Hour to end in (hh:mm) format. The range is from 0 to 23.
offset	Minutes offset (see Table 2-2) from Coordinated Universal Time (UTC) The range is from 0 to 59.
recurring	Configures the recurring summer time.
1-4	Configures the starting week number. The range is from 1 to 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 to start. The range is from Monday to Friday.
startmonth	Month to start. The range is from January through December.
starthour	Hour to start in hh:mm format. The range is from 0 to 23.
endweekday	Weekday to end. The range is from Monday to Friday
endmonth	Month to end. The range is from January through December.
endhour	Hour to end in hour:minute (hh:mm) format. The range is from 0 to 23.
offset	Minutes offset (see Table 2-2) from UTC. The range is from 0 to 59.
timezone	Configures the standard time zone.
timezone	Name of the time zone.

hoursoffset	Hours offset (see Table 2-2) from UTC. The range is from –23 to +23.
minutesoffset	Minutes offset (see Table 2-2) from UTC. The range is from 0 to 59.

Defaults

None

Command Modes

Global configuration (config) mode.

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** command in EXEC configuration mode. The UTC and local time are displayed with the **show clock detail** command in EXEC configuration mode.

Use the **clock** *timezone offset* command to specify a time zone, where *timezone* is the desired time zone entry from Table 2-2 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, Table 2-2. When you use a time zone entry from Table 2-2, the system is automatically adjusted for daylight saving time.

Note If you change the local time on the device, you must change the BIOS clock time as well; otherwise, the timestamps on the error logs are not synchronized. Changing the BIOS clock is required because the kernel does not handle time zones.

The offset (ahead or behind) UTC in hours, as displayed in Table 2-2, 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.

Table 2-2 lists all the standard time zones that you can configure on a content delivery engine (CDE) and the offset from Coordinated Universal Time (UTC) for each standard time zone. The offset (ahead or behind) UTC in hours, as displayed in Table 2-2, 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 The time zone entry is case sensitive and must be specified in the exact notation listed in the following time zone table. When you use a time zone entry from the following time zone table, the system is automatically adjusted for daylight saving time.

Table 2-2 List of Standard Time Zones and Offsets from UTC

Time Zone	Offset from UTC
Africa/Abidjan	0
Africa/Accra	0
Africa/Addis_Ababa	+3
Africa/Algiers	+1
Africa/Asmera	+3
Africa/Bamako	0
Africa/Bangui	+1
Africa/Banjul	0
Africa/Bissau	0
Africa/Blantyre	+2
Africa/Brazzaville	+1
Africa/Bujumbura	+2
Africa/Cairo	+2
Africa/Casablanca	0
Africa/Ceuta	+1
Africa/Conakry	0
Africa/Dakar	0
Africa/Dar_es_Salaam	+3
Africa/Djibouti	+3
Africa/Douala	+3
Africa/El_Aaiun	+1
Africa/Freetown	0
Africa/Gaborone	+2
Africa/Harare	+2
Africa/Johannesburg	+2
Africa/Kampala	+3
Africa/Khartoum	+3
Africa/Kigali	+2
Africa/Kinshasa	+1
Africa/Lagos	+1
Africa/Libreville	+1
Africa/Lome	0
Africa/Luanda	+1
Africa/Lubumbashi	+2
Africa/Lusaka	+2
Africa/Malabo	+1

Table 2-2 List of Standard Time Zones and Offsets from UTC (continued)

Time Zone	Offset from UTC
Africa/Maputo	+2
Africa/Maseru	+2
Africa/Mbabane	+2
Africa/Mogadishu	+3
Africa/Monrovia	0
Africa/Nairobi	+3
Africa/Ndjamena	+1
Africa/Niamey	+1
Africa/Nouakchott	0
Africa/Ouagadougou	0
Africa/Porto-Novo	+1
Africa/Sao_Tome	0
Africa/Timbuktu	0
Africa/Tripoli	+2
Africa/Tunis	+1
Africa/Windhoek	+1
America/Anguilla	–4
America/Antigua	–4
America/Araguaina	–3
America/Aruba	–4
America/Asuncion	–4
America/Barbados	–4
America/Belem	–3
America/Belize	–6
America/Boa_Vista	–4
America/Bogota	–5
America/Boise	–7
America/Buenos_Aires	–3
America/Cambridge_Bay	–7
America/Cancun	–6
America/Caracas	–4
America/Catamarca	–3
America/Cayenne	–3
America/Cayman	–5
America/Chihuahua	–7
America/Cordoba	–3

Table 2-2 List of Standard Time Zones and Offsets from UTC (continued)

Time Zone	Offset from UTC
America/Costa_Rica	–6
America/Cuiaba	–4
America/Curacao	–4
America/Dawson	–8
America/Dawson_Creek	–7
America/Dominica	–4
America/Eirunepe	–5
America/El_Salvador	–6
America/Fortaleza	–3
America/Glace_Bay	–4
America/Godthab	–3
America/Goose_Bay	–4
America/Grand_Turk	–5
America/Grenada	–4
America/Guadeloupe	–4
America/Guatemala	–6
America/Guayaquil	–5
America/Guyana	–4
America/Hermosillo	–7
America/Indiana/Marengo	–5
America/Indiana/Vevay	–5
America/Indiana/Indianapolis	–5
America/Indiana/Knox	–5
America/Inuvik	–7
America/Iqaluit	–5
America/Jujuy	–3
America/Juneau	–9
America/Kentucky/Monticello	–5
America/Kentucky/Louisville	–5
America/La_Paz	–4
America/Lima	–5
America/Louisville	–8
America/Maceio	–3
America/Managua	–6
America/Martinique	–4
America/Mendoza	–3

Table 2-2 List of Standard Time Zones and Offsets from UTC (continued)

Time Zone	Offset from UTC
America/Menominee	–6
America/Merida	–6
America/Miquelon	–3
America/Monterrey	–6
America/Montevideo	–3
America/Montserrat	–4
America/Nassau	–5
America/Nipigon	–5
America/Nome	–9
America/Panama	–5
America/Pangnirtung	–3
America/Paramaribo	–3
America/Port-au-Prince	–5
America/Port_of_Spain	–4
America/Porto_Velho	–4
America/Rainy_River	–6
America/Rankin_Inlet	–6
America/Recife	–3
America/Rosario	–3
America/Santo_Domingo	–4
America/Scoresbysund	–1
America/St_Kitts	–4
America/St_Lucia	–4
America/St_Vincent	–4
America/Swift_Current	–6
America/Tegucigalpa	–6
America/Thule	–4
America/Thunder_Bay	–5
America/Tortola	–4
America/Virgin	–4
America/St_Thomas	–4
America/Yakutat	–9
America/Yellowknife	–7
America/Porto_Acre	–5
America/Rio_Branco	–5
America/Noronha	–2

Table 2-2 List of Standard Time Zones and Offsets from UTC (continued)

Time Zone	Offset from UTC
America/Sao_Paulo	–3
America/Manaus	–4
America/Winnipeg	–6
America/Montreal	–5
America/Edmonton	–7
America/St_Johns	–3.30
America/Vancouver	–8
America/Whitehorse	–8
America/Santiago	–4
America/Havana	–5
America/Jamaica	–5
America/Ensenada	–8
America/Tijuana	–8
America/Mazatlan	–7
America/Mexico_City	–6
America/Puerto_Rico	–4
America/Halifax	–4
America/Regina	–6
America/Anchorage	–9
America/Adak	–10
America/Atka	–10
America/Phoenix	–7
America/Chicago	–6
America/Fort_Wayne	–5
America/Indianapolis	–5
America/Knox_IN	–5
America/Detroit	–7
America/Denver	–5
America/Shiprock	–7
America/Los_Angeles	–8
America/New_York	–5
Antarctica/Casey	+8
Antarctica/Davis	+7
Antarctica/DumontDUrville	+10
Antarctica/Mawson	+6
Antarctica/Palmer	–4

Table 2-2 List of Standard Time Zones and Offsets from UTC (continued)

Time Zone	Offset from UTC
Antarctica/South_Pole	+12
Antarctica/McMurdo	+12
Antarctica/Syowa	+3
Antarctica/Vostok	+6
Arctic/Longyearbyen	+1
Asia/Aden	+3
Asia/Almaty	+6
Asia/Amman	+2
Asia/Anadyr	+12
Asia/Aqtau	+4
Asia/Aqtobe	+5
Asia/Ashkhabad	+5
Asia/Ashgabat	+5
Asia/Baghdad	+3
Asia/Bahrain	+3
Asia/Baku	+4
Asia/Bangkok	+7
Asia/Beirut	+2
Asia/Bishkek	+5
Asia/Brunei	+8
Asia/Calcutta	+5.30
Asia/Chungking	+8
Asia/Colombo	+6
Asia/Damascus	+2
Asia/Dhaka	+6
Asia/Dacca	+6
Asia/Dili	+9
Asia/Dubai	+4
Asia/Dushanbe	+5
Asia/Gaza	+2
Asia/Harbin	+8
Asia/Hovd	+7
Asia/Irkutsk	+8
Asia/Jakarta	+7
Asia/Jayapura	+9
Asia/Kabul	+4.30

Table 2-2 List of Standard Time Zones and Offsets from UTC (continued)

Time Zone	Offset from UTC
Asia/Kamchatka	+12
Asia/Karachi	+5
Asia/Kashgar	+8
Asia/Katmandu	+5.45
Asia/Krasnoyarsk	+7
Asia/Kuala_Lumpur	+8
Asia/Kuching	+8
Asia/Kuwait	+3
Asia/Macao	+8
Asia/Magadan	+11
Asia/Manila	+8
Asia/Muscat	+4
Asia/Novosibirsk	+6
Asia/Omsk	+6
Asia/Phnom_Penh	+7
Asia/Pontianak	+7
Asia/Pyongyang	+9
Asia/Qatar	+3
Asia/Rangoon	+6.30
Asia/Riyadh	+3
Asia/Saigon	+7
Asia/Samarkand	+5
Asia/Tashkent	+5
Asia/Tbilisi	+3
Asia/Thimphu	+6
Asia/Thimbu	+6
Asia/Ujung_Pandang	+8
Asia/Ulan_Bator	+8
Asia/Ulaanbaatar	+8
Asia/Urumqi	+8
Asia/Vientiane	+7
Asia/Vladivostok	+10
Asia/Yakutsk	+9
Asia/Yekaterinburg	+5
Asia/Yerevan	+4
Asia/Nicosia	+2

Table 2-2 List of Standard Time Zones and Offsets from UTC (continued)

Time Zone	Offset from UTC
Asia/Hong_Kong	+8
Asia/Tehran	+3.30
Asia/Jerusalem	+2
Asia/Tel_Aviv	+2
Asia/Tokyo	+9
Asia/Riyadh87	+3.07
Asia/Riyadh88	+3.07
Asia/Riyadh89	+3.07
Asia/Shanghai	+8
Asia/Taipei	+8
Asia/Seoul	+9
Asia/Singapore	+8
Asia/Istanbul	+2
Atlantic/Azores	–1
Atlantic/Bermuda	–4
Atlantic/Canary	0
Atlantic/Cape_Verde	–1
Atlantic/Faeroe	0
Atlantic/Madeira	0
Atlantic/South_Georgia	–2
Atlantic/St_Helena	0
Atlantic/Stanley	–4
Atlantic/Jan_Mayen	+1
Atlantic/Reykjavik	0
Australia/Lindeman	+10
Australia/Lord_Howe	+10.30
Australia/LHI	+10.30
Australia/North	+9.30
Australia/Darwin	+9.30
Australia/Queensland	+10
Australia/Brisbane	+10
Australia/South	+9.30
Australia/Adelaide	+9.30
Australia/Sydney	+10
Australia/ACT	+10
Australia/Canberra	+10

Table 2-2 List of Standard Time Zones and Offsets from UTC (continued)

Time Zone	Offset from UTC
Australia/NSW	+10
Australia/Tasmania	+10
Australia/Hobart	+10
Australia/Victoria	+10
Australia/Melbourne	+10
Australia/West	+8
Australia/Perth	+8
Australia/Yancowinna	+9.30
Australia/Broken_Hill	+9.30
Brazil/Acre	–5
Brazil/DeNoronha	–2
Brazil/East	–3
Brazil/West	–4
CET	+1
Canada/Central	–6
Canada/Eastern	–5
Canada/Mountain	–7
Canada/Newfoundland	–3.30
Canada/Pacific	–8
Canada/Yukon	–8
Canada/Atlantic	–4
Canada/East-Saskatchewan	–6
Canada/Saskatchewan	–6
Chile/Continental	–4
Chile/EasterIsland	–6
Cuba	–5
EET	+2
Egypt	+2
Europe/Amsterdam	+1
Europe/Andorra	+1
Europe/Athens	+2
Europe/Belfast	0
Europe/Berlin	+1
Europe/Brussels	+1
Europe/Bucharest	+2
Europe/Budapest	+1

Table 2-2 List of Standard Time Zones and Offsets from UTC (continued)

Time Zone	Offset from UTC
Europe/Copenhagen	+1
Europe/Dublin	0
Europe/Gibraltar	0
Europe/Helsinki	+2
Europe/Kaliningrad	+2
Europe/Kiev	+2
Europe/London	0
Europe/Luxembourg	+1
Europe/Madrid	+1
Europe/Malta	+1
Europe/Minsk	+2
Europe/Monaco	+1
Europe/Nicosia	+2
Europe/Oslo	+1
Europe/Paris	+1
Europe/Prague	+1
Europe/Bratislava	+1
Europe/Riga	+2
Europe/Samara	+4
Europe/Simferopol	+2
Europe/Sofia	+2
Europe/Stockholm	+1
Europe/Tallinn	+2
Europe/Tirane	+1
Europe/Tiraspol	+2
Europe/Chisinau	+2
Europe/Uzhgorod	+2
Europe/Vaduz	+1
Europe/Vatican	+1
Eire	0
GB-Eire	0
GB	0
Greenwich	0
GMT	0
GMT+0	0
GMT-0	0

Table 2-2 List of Standard Time Zones and Offsets from UTC (continued)

Time Zone	Offset from UTC
GMT0	0
Hongkong	+8
Iceland	0
Indian/Antananarivo	+3
Indian/Chagos	+6
Indian/Christmas	+7
Indian/Cocos	+6.30
Indian/Comoro	+3
Indian/Kerguelen	+5
Indian/Mahe	+4
Indian/Maldives	+5
Indian/Mauritius	+4
Indian/Mayotte	+3
Indian/Reunion	+4
Iran	+3.30
Israel	+2
Jamaica	–5
Japan	+9
Libya	+2
MET	+1
Mexico/BajaNorte	–8
Mexico/BajaSur	–7
Mexico/General	–6
Mideast/Riyadh87	+3.07
Mideast/Riyadh88	+3.07
Mideast/Riyadh89	+3.07
PRC	+8
Pacific/Apia	–11
Pacific/Auckland	+12
Pacific/Chatham	+12.45
Pacific/Easter	–6
Pacific/Efate	+11
Pacific/Enderbury	+13
Pacific/Fakaofo	–10
Pacific/Fiji	+12
Pacific/Funafuti	+12

Table 2-2 List of Standard Time Zones and Offsets from UTC (continued)

Time Zone	Offset from UTC
Pacific/Galapagos	–6
Pacific/Guadalcanal	+11
Pacific/Guam	+10
Pacific/Johnston	–10
Pacific/Kiritimati	+14
Pacific/Kosrae	+11
Pacific/Kwajalein	+12
Pacific/Majuro	+12
Pacific/Marquesas	–9.30
Pacific/Midway	–11
Pacific/Nauru	+12
Pacific/Niue	–11
Pacific/Norfolk	+11.30
Pacific/Noumea	+11
Pacific/Palau	+9
Pacific/Ponape	+11
Pacific/Port_Moresby	+10
Pacific/Rarotonga	–10
Pacific/Saipan	+10
Pacific/Tahiti	–10
Pacific/Tarawa	+12
Pacific/Tongatapu	+13
Pacific/Truk	+10
Pacific/Wake	+12
Pacific/Wallis	+12
Pacific/Yap	+10
Pacific/Pitcairn	–8
Pacific/Gambier	–9
Pacific/Honolulu	–10
Pacific/Pago_Pago	–11
Pacific/Samoa	–11
NZ	+12
NZ-CHAT	+12.45
Kwajalein	+12
Poland	+1
Portugal	0

Table 2-2 List of Standard Time Zones and Offsets from UTC (continued)

Time Zone	Offset from UTC
ROC	+8
ROK	+9
Singapore	+8
Turkey	+2
UCT	0
US/Alaska	–9
US/Aleutian	–10
US/Arizona	–7
US/Central	–6
US/East-Indiana	–5
US/Hawaii	–10
US/Indiana-Starke	–5
US/Michigan	–5
US/Mountain	–7
US/Pacific	–8
US/Samoa	–11
US/Eastern	–5
MST	+7
CST6CDT	–6
EST	–5
HST	–10
MST7MDT	+7
Navajo	–7
PST8PDT	–8
W-SU	+3
WET	0
Zulu	0
UTC	0
Universal	0
EST5EDT	–5

Examples

The following example shows how to specify 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 shows how to configure 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 shows how to configure daylight saving time:

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

Related Commands

Command	Description
clock	To set the summer daylight saving time and time zone for display purposes.
show clock detail	Displays the Coordinated Universal Time (UTC) and local time.

cms (EXEC configuration)

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

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 VOSM.
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 a VDS-OS network device.
identity	Specifies the identity of the recovered device.
word	Identity of the recovered device.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The VDS-OS network is a collection of SR, SE and VOSM nodes. One primary VOSM retains the VDS-OS network settings and provides other VDS-OS network nodes with updates. Communication between nodes occurs over secure channels using the Secure Shell Layer (SSL) protocol, where each node on the VDS-OS 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 VOSM to contact the primary VOSM 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 VOSM and activated, it appears as Pending in the VOSM 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 a VDS-OS network, it must first be registered and then activated. The **cms enable** command automatically registers the node in the database management tables and enables the CMS. The node sends its attribute information to the VOSM over the SSL protocol and then stores the new node information. The VOSM 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 VOSM GUI.

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

Note The **cms deregister** command cleans up the database automatically. You do not need to use the **cms database delete** command. If the deregistration fails, the best practice is to resolve any issues that caused the deregistration failure; for example, the Service Engine is the Content Acquirer of a delivery service and cannot be deleted or deactivated. Assign a different SE as the Content Acquirer in each delivery service where this SE is assigned as the Content Acquirer and try the **cms deregister** command again.

To back up the existing management database for the VOSM, 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, specify the device recovery key that you configured in the Modifying Config Property, System.device.recovery.key window of the VOSM GUI.

Use the **lcm** command to configure local or central management (LCM) on a VDS-OS network device. The LCM feature allows settings configured using the device CLI or GUI to be stored as part of the VDS-OS 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 VOSM detects the configuration changes that you made on these devices using CLIs and sends the changes to the primary VOSM.

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

If LCM is disabled, the settings configured through the VOSM GUI 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 VOSM 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 VOSM, the local device configuration is applicable until the VOSM 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 VOSM GUI triggers a full update). When the VOSM requests a full update from the device, the VOSM settings overwrite the local device settings.

The **cms deregister force** command should be used only as the last option, because the VOSM does not know about the device being removed. When executing the **cms deregister force** command, take note of any messages stating that the deregistration failed and make sure to resolve them before reregistering the device with the same VOSM or registering the device to another VOSM. The **cms deregister force** command forces the deregistration to continue.

Examples

The following example shows how to back up the database management tables:

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

The following example shows how to validate the database management tables:

```
VOSM# 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 VOSM
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 VOSM 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 VOSM
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_VOSM.
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-VOSM 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 VOSM GUI:

```
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 VOSM
10.107.192.168
There are no SE devices in CDN
register: Registration failed.
ServiceEngine#
```

Related Commands

Command	Description
cms enable	Enables the CMS.
show cms	Displays the CMS protocol, embedded database content, maintenance status, and other information.

cms (global configuration)

To schedule maintenance and enable the Centralized Management System (CMS) on a given node, use the **cms** command in global configuration mode. 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. The range is from 0 to 23:0 to 59 in hh:mm format.
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 for when making a connection.
5-1800	Timeout period, in seconds. The default for the VOSM is 30; the default for the SE and the SR is 180.
incoming-wait	Specifies the maximum time to wait for a client response.
10-600	Timeout period, in seconds. The default is 30.
transfer	Specifies the maximum time to allow a connection to remain open.
10-7200	Timeout period, in seconds. The default is 300.

Defaults

database maintenance regular: enabled

database maintenance full: enabled

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

incoming wait: 30 seconds

transfer: 300 seconds

Command Modes

Global configuration (config) mode.

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 runs only 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 stops only 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 VDS-OS network and to disable communication between two multicast senders.

Examples

The following example shows how to schedule 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 VOSM
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_VOSM.
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-VOSM 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 VOSM. Any configuration changes
made via CLI on this device will be overwritten if they conflict with settings on the
VOSM.
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 VOSM UI.
management services enabled
ServiceEngine(config)#
```

Related Commands

Command	Description
cms database	Creates, backs up, deletes, restores, or validates the CMS-embedded database management tables or files.
show cms	Displays the CMS protocol, embedded database content, maintenance status, and other information.

configure

To enter global configuration mode, use the **configure** command in EXEC configuration mode.

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 keywords or arguments.

Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to enable global configuration mode:

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

Related Commands

Command	Description
end	Exits configuration and privileged EXEC configuration modes.
exit	Exits from interface, global configuration, or privileged EXEC configuration modes.
show running-config	Displays the current operating configuration.
show startup-config	Displays the startup configuration.

content-origin

To support multiple origin services within a content origin, use the **content-origin** command in global configuration mode. To remove configured content origin, use the no form of this command.

content-origin request-fqdn *domain* **config-url** *url* [**username** *username* **password** *password*]

no content-origin request-fqdn *domain* **config-url** *url* [**username** *username* **password** *password*]

Syntax Description

request-fqdn	Configures the request fully qualified domain name (FQDN).
domain	Domain of the request FQDN. Domain size range should be between 1to 255 characters.
config-url	URL of the content origin configuration file.
url	URL name.
username	Configures a username to access configuration file.
username	Specifies a username.
password	Configures a password to access configuration file.
password	Specifies a password.

Defaults

None

Command Modes

Global configuration mode.

Usage Guidelines

Previously, only one origin service per content origin was allowed and the same origin service could not be shared across multiple content origins. Users had to create delivery services or content origins and different content origin domain names resolving to same IP addresses of the origin service. This created much overhead during deployment. The **content-origin** command supports multiple origin services within a content origin and allows users to share single origin services across multiple delivery service or content origins.

Examples

The following example shows how to support multiple origin services within a content origin:

```
ServiceEngine# content-origin request-fqdn xxx.com config-url
http://171.XX.XX.XXX/VDS-OSorigin.xml username admin password default
```

Related Commands

Command	Description
show content-origin	Displays information about the Network-Attached Storage (NAS) mount.

copy

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

copy cdnfs disk *url sysfs-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**}

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

copy system-status disk *filename*

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

Syntax Description

cdnfs	Copies a file from the CDS network file system (CDNFS) to the system file system (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.
disk	Copies a local disk file.
ftp	Copies to a file on a File Transfer Protocol (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 after 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 (nonvolatile random-access memory [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. The default is 80.
port-num	HTTP server port number. The range is from 1 to 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. The range is from 1 to 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 (nonvolatile random-access memory [NVRAM]).
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.
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 Trivial File Transfer Protocol (TFTP) server. Use the complete pathname.

Defaults

HTTP server port: 80

Default working directory for sysfs files: /local1

Command Modes

EXEC configuration mode.

Usage Guidelines

The **copy cdnfs** command in EXEC configuration mode copies data files from of the CDNFS to the sysfs for further processing. For example, you can use the **install** *imagefilename* command in EXEC configuration mode 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 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 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 copies technical support information to a a sysfs partition.

Related Commands

Command	Description
install	Installs a new version of the caching application.
reload	Halts a device and performs a cold restart.
show running-config	Displays the current operating configuration.
show startup-config	Displays the startup configuration.
write	Writes or erases the startup configurations to NVRAM or to a terminal session, or writes the Management Information Base (MIB) persistence configuration to disk.

core-dump

To configure a coredump file, use the **core-dump** command in EXEC configuration mode.

core-dump {backtrace {all| *word*} | **service** {**acquisition force | cms force | distribution force | dns force | rtspg force | service-router force**}}

Syntax Description

backtrace	Displays the backtrace of a coredump file.
all	Displays the backtraces of all core files.
word	Specifies the name of the core file.
service	Creates a core dump of a specific service.
acquisition	Specifies acquisition services.
force	Forces a core dump of the service.
cms	Specifies cms services.
distribution	Specifies distribution services.
dns	Specifies dns services.
rtspg	Specifies rtspg services.
service-router	Specifies service-router services.

Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to display the backtrace of all coredump files:

```
ServiceEngine# core backtrace al
```

cpfile

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

cpfile *oldfilename newfilename*

Syntax Description

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

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use this command to create a copy of a file. Only system file system (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

Command	Description
copy	Copies the configuration or image files to and from the CD-ROM, flash memory, disk, or remote hosts.
dir	Displays the files in a long-list format.
lls	Displays the files in a long-list format.
ls	Lists the files and subdirectories in a directory.
mkfile	Makes a file (for testing).
rename	Renames a file.
rmdir	Removes a directory.

debug

To monitor and record caching application functions, use the **debug** command in EXEC configuration mode. To disable these functions, 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

debug all: default logging level is ERROR.

Command Modes

EXEC configuration mode.

Usage Guidelines

We recommend that you use the **debug** command only at the direction of Cisco Technical Assistance Center (TAC) because the SE performance is affected when you enter the **debug** command.

You can use the **logging disk priority debug** 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, disable the debugging functions by using the **undebug** command (see the "undebug" section on page 2-428 section for more details), and reset the level of logging disk priority to any other setting that you want (for example, **notice** priority).

Table 2-3 shows valid values for the **debug** command options.

Table 2-3 debug Command Options

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

Table 2-3 debug Command Options

authentication	Debugs authentication.
user	Debugs the user login against the system authentication.
capturecontroller	Debug the Capture Controller
error	Sets the debug level to error.
trace	Sets the debug level to trace.
cdnfs	Debugs the CNNFS.
cds-origin-manager	Debugs the CDN Origin Manager.
error	Sets the debug level to error.
trace	Sets the debug level to trace.
cli	Debugs the CLI command.
all	Debugs all CLI commands.
bin	Debugs the CLI command binary program.
pam	Debugs the CLI command pam.
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 Distributed filesystem (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 Dynamic Host Configuration Protocol (DHCP).
emdb	Debugs the embedded database.
level	(Optional) Debug level.
(0-16)	Debug level 0 through 16.
http	Debugs HTTP.
service-router	Debugs the HTTP Service Router.
logging	Debugs logging.
all	Debugs all logging functions.

Table 2-3 debug Command Options

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	Domain Name System (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.
log-directory	Memory allocation debugging log directory.
word	Directory path name.
ntp	Debugs Network Time Protocol (NTP).
rpc	Displays the remote procedure call (RPC) logs.
detail	Displays the RPC logs of priority *detail* level or higher.
trace	Displays the RPC logs of priority *trace* level or higher.
service-router	Debug commands for the Service Router.
servicemonitor	Debug commands for the service monitor.
snmp	Debugs Simple Network Management Protocol (SNMP).
agent	SNMP agent debug.
all	Debugs all SNMP functions.
cli	Debugs the SNMP CLI.
main	Debugs the SNMP main.
mib	Debugs the SNMP Management Information Base (MIB).
traps	Debugs the SNMP traps.
standby	Debugs standby functions.
all	(Optional) Debugs all standby functions.

Table 2-3 debug Command Options

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 File Transfer Protocol (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.
web-engine	Web Engine debug commands.
error	Sets the debug level to error.
trace	Sets the debug level to trace.
wi	Debugs the web interface.

Debugging Keywords

All modules have **debug error** as the default level if they support the **error** keyword; however, when you execute the **show debug** command, the error does not display.

Some modules have two debugging keywords (**error** and **trace**), but you cannot enable both at the same time. See the table above to identify commands with only the **error** and **trace** keywords.

Some modules have the **all** keyword through which you can enable both the **error** and **trace** keywords at the same time. This results in *debug set to everything*. See Table 2-3 to identify commands with the **all** keyword.

Note When debugging is set to trace level, it uses a lot of the CPU on the SE to handle error log writing. When writing the trace-level error logs reaches 100 percent of the CPU usage, 504 timeout error messages start to occur. Therefore, trace-level error logging should not be enabled in production systems.

Debugging Cdnfs

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

Related Commands

Command	Description
show debugging	Displays the state of each debugging option.
undebug	Disables the debugging functions (see also **debug**).

delfile

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

delfile *filename*

Syntax Description

filename	Name of the file to delete.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use this command to remove a file from a system file system (sysfs) partition.

Examples

The following example shows how to delete a file:

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

Related Commands

Command	Description
cpfile	Copies a file.
deltree	Deletes a directory and its subdirectories.
mkdir	Creates a directory.
mkfile	Creates a file (for testing).
rmdir	Removes a directory.

deltree

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

deltree *directory*

Syntax Description

directory	Name of the directory tree to delete.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use this command to remove a directory and all files within the directory from the Service Engine (SE) system file system (sysfs). 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

Command	Description
delfile	Deletes a file.
mkdir	Creates a directory.
mkfile	Creates a file (for testing).
rmdir	Removes a directory.

device

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

device mode {**service-engine** | **service-router** | **virtual-origin-system-manager**}

no device mode {**service-engine** | **service-router** | **virtual-origin-system-manager**}

Syntax Description

mode	Sets the mode of operation of a device to VOSM, SE or SR.
service-engine	Configures the device operation mode as an SE.
service-router	Configures the device operation mode as an SR.
virtual-origin-system-manager	Configures the device to function as a Virtual Origin System Manager.

Defaults

The default device operation mode is SE.

Command Modes

Global configuration (config) mode.

Usage Guidelines

A VOSM is the content management and device management station of a VDS-OS 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 VDS-OS 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 a VDS-OS network, each serving a local set of clients. IP/TV brings movie-quality video over enterprise networks to the desktop of the VDS-OS 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 VOSM (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 VDS-OS network-related applications and services, use the **cms enable** command. Use the **no** form of this command to disable the VDS-OS network.

All VDS-OS devices ship from the factory as SEs. Before configuring network settings for VOSMs and SRs using the CLI, 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** 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 VOSM, you may need to reconfigure the system file system (sysfs). However, SRs and VOSMs do not require any disk space other than sysfs. When you change the device mode to an SR or a VOSM, 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 VDS-OS network device.

If you are changing the device mode of an SR or a VOSM back to an SE, 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 VOSM, SR and SE modes:

```
ServiceEngine(config)# device mode virtual-origin-system-manager

VOSM(config)# device mode service-router

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

Related Commands

Command	Description
show device-mode	Displays the configured or current mode of a VOSM, SE or SR device.

dir

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

dir [*directory*]

Syntax Description

directory	(Optional) Name of the directory to list.

Defaults

None

Command Modes

EXEC configuration mode.

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

Command	Description
lls	Displays the files in a long list format.
ls	Lists the files and subdirectories in a directory.

disable

To turn off privileged command in EXEC configuration mode, use the **disable** command in EXEC configuration mode.

disable

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

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

Examples

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

```
ServiceEngine# disable
ServiceEngine>
```

Related Commands

Command	Description
enable	Accesses the privileged EXEC commands.

disk (EXEC configuration)

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

disk {**erase** *diskname* | **mark** *diskname* {**bad** | **good**} | **policy apply** | **recover-cdnfs-volumes** | **recover-system-volumes** | **repair** *diskname* **sector** *sector_address_in_decimal* | **unuse** *diskname*}

Syntax Description

erase	Erases drive (DANGEROUS).
diskname	Name of the disk to be erased (disk00, disk01, and so on).
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.
policy	Applies disk policy management.
apply	Invokes the disk policy manager for a disk.
recover-cdnfs-volumes	Erases all CDS network file system (CDNFS) volumes and reboots.
recover-system-volumes	Erases all SYSTEM and SYSFS volumes.
repair	Repairs the drive.
diskname	Name of the disk to be repaired (disk00, disk01, and so on).
sector	Repairs a sector that cannot be corrected.
sector_address_in_decimal	Name of the sector address in decimal.
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

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The disk space in the CDS software is allocated on a per-file system basis, rather than on a per-disk basis.

The CDNFS amounts are reported by the actual usable amounts of storage for applications. Because of 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 disk details** command.

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

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

After upgrading, the disk space allocation remains the same as previously configured.

Remapping of Bad Sectors on Disk Drives

The **disk erase** command in EXEC configuration mode performs a low-level format of the Small Computer Systems Interface (SCSI) or Serial Advanced Technology Attachment (SATA) disks. This command erases all the content on the disk.

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

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

Note SCSI and SATA drives can be reformatted.

Erasing Disk Drives

The **disk erase** command replaced the **disk reformat** command. This command erases all the content on the disk. The sequence to erase a disk with the **disk erase** and then use the **disk policy apply** commands. If a disk drive continues to report a failure after you have used the **disk erase** command, you must replace the disk drive.

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

Disk Hot Swapping

A new disk is recognized and the RAID is rebuilt when the device is rebooted. After inserting the new disk, enter the **disk policy apply** command to force the VDS-OS software to detect the new disk and rebuild the RAID.

Note RAID is not supported for generic hardware (UCS servers). These systems have a single un-RAIDed system disk. Any disk replacement requires that the system first be taken off-line.

The disk policy's design, when adding new disks, is to always favor safety. If when a new disk is added, the disk manager detects “degraded” or “bad” system volumes, the new disk is used to repair the system volumes. Thus, the disk manager always strives to have two disks allocated to the system volumes. If when a new disk is added, the system volumes are “normal” or “syncing,” the new disk is added to the cdnfs volume.

Note For the CDE220-2S3i,and the CDE220-2S3, because the system disks are internal drives, if the system disk is “bad,” the CDE should be replaced.

Repairing a Disk

The **disk repair** command re pairs the bad sector, including the proximal sectors. All data on the drive is lost, but the sectors are repaired and available for data storage again. This command provides equivalent functionality as the repair-disk utility. The disk repair command takes approximately three hours to complete per disk; after the repair disk command completes, reboot the SE to ensure all VDS-OS software services are functioning correctly.

Caution The device should be off-line before running the **disk repair** command. Because this command involves complex steps, we recommend you contact Cisco Technical Support before running this command.

The **disk repair** command not only repairs the bad sectors, but reformats the entire drive, so all data on the drive is lost. The difference between the **disk repair** command and the **disk erase** command is that the **disk erase** command only re-initializes the file system and does not repair bad sectors.

A minor alarm is set when an LSE is detected. After the sector is repaired with the disk repair command, the alarm is turned off.

```
Minor Alarms:
-------------
     Alarm ID             Module/Submodule     Instance
     -------------------- -------------------- ------------------------
   1 badsector            sysmon               disk11
     May 19 20:40:38.213 UTC, Equipment Alarm, #000003, 1000:445011
     "Device: /dev/sdl, 1 Currently unreadable (pending) sectors"
```

Stopping Applications from Using a Disk Drive

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

Note When executing the **disk unuse** command, any applications using the disk will be terminated. Off-line the device before executing this command.

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

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

Examples

The following example shows how to repair the sector 4660 on disk 02:

```
ServiceEngine# disk repair disk02 sector 4660
```

Note A system disk cannot be unused in a non-RAID system (generic/ucs).

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
To safely remove a RAID SYSTEM disk, the entire drive must be erased. This
operation has little effect on the RAID-ed SYSTEM volumes, as their data can
be resynced. However, because the drive also contains non-RAID CDNFS
data, it will result in loss of all CDNFS data for this drive!
Unuse disk01, erasing all CDNFS data? (Yes/No): yes
disk01 is now unused.
All partitions on disk01 have been erased.

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 view disk details:

```
ServiceEngine# show disk details
disk00: Normal (h02 c00 i00 l00 - mptsas) 476940MB(465.8GB)
disk00/01: SYSTEM 5120MB(5.0GB) mounted internally
disk00/02: SYSTEM 2560MB(2.5GB) mounted internally
disk00/04: SYSTEM 1536MB(1.5GB) mounted internally
disk00/05: SYSFS 32767MB(32.0GB) mounted at /local1
disk00/06: CDNFS 434948MB(424.8GB) mounted internally
disk01: Normal (h02 c00 i01 l00 - mptsas) 476940MB(465.8GB)
Unallocated: 476940MB(465.8GB)
disk02: Normal (h02 c00 i02 l00 - mptsas) 476940MB(465.8GB)
disk02/01: CDNFS 476932MB(465.8GB) mounted internally
```

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

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

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 %
```

The following example shows how to erase all CDNFS volumes and reboot the SE:

```
ServiceEngine# disk recover-cdnfs-volumes
This will erase all CDNFS volumes.
Any applications using CDNFS, including streaming applications, will be killed and the
system will be rebooted.
Please make sure you have offloaded the SE on the VOSM GUI so the SR is no longer sending
traffic to this SE.
Are you sure you want to proceed? [no] yes Are you really sure you want to proceed to
recover and reload? [yes/no] yes

Stopping all services (this may take several minutes)...
diskman will now recover CDNFS volumes...
CDNFS recovery complete, rebooting now...
```

Related Commands

Command	Description
disk (global configuration mode)	Configures how the disk errors should be handled.
show cdnfs	Displays the CDS network file system information.
show disk	Displays the disk configurations.
show disk details	Displays more detailed Self Monitoring, Analysis, and Reporting Technology (SMART) disk monitoring information.
show statistics	Displays statistics by module.

disk (global configuration)

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

disk error-handling {**bad-sectors-mon-period** *minutes* | **reload** | **threshold** {**alarm-bad-sectors** *bad-sectors* | **alarm-remapped-sectors** *remapped-sectors* | **bad-sectors** bad-sectors | **errors** errors}}

no disk error-handling {bad-sectors-mon-period minutes | reload | threshold {alarm-bad-sectors bad-sectors | alarm-remapped-sectors remapped-sectors | bad-sectors bad-sectors | errors errors}}

Syntax Description

error-handling	Configures disk error handling.
bad-sectors-mon-period	Active bad sectors monitoring period (minutes).
minutes	Default value is 1440 minutes (24 hours); 0 disables sector monitoring. The range is from 0 to 525600.
reload	Whether to reload system if SYSFS disk(s) have problems.
threshold	Configure disk error handling thresholds.
alarm-bad-sectors	Configures the bad sector alarm threshold.
bad-sectors	Number of bad sectors allowed before the disk is marked as bad. The range is from 0 to 100. The default value is 15. The value 0 means that the disk should never be marked as bad.
alarm-remapped-sectors	Configure SMARTinfo remapped sectors alarm threshold (hard drives only).
remapped-sectors	Number of remapped sectors before alarm is triggered. Default value is 128 (hard drives only). The range is from 0 to 8192.
bad-sectors	Configure number of allowed (Active) bad sectors before disk is marked bad.  **Note** Only applies to bad sectors detected since system boot.
bad-sectors	Number of bad sectors allowed before disk is marked bad. Default value is 30; 0 means the disk is never mark bad. The range is from 0 to 100.
errors	Configure number of allowed disk errors before marking disk bad.  **Note** Only applies to disk or sector errors detected since system boot.
errors	The number of disk errors allowed before the disk is marked bad. Default value is 500; 0 means never mark disk bad. The range is from 0-100000.

Defaults

Bad sector minutes: 1440

Bad sectors alarm: 15

Remapped sectors: 128

Disk bad sectors: 30

Errors: 500

Command Modes

Global configuration (config) mode.

Usage Guidelines

To operate properly, the SE must have critical disk drives. A critical disk drive is the first disk drive that also contains the first system file system (sysfs) partition. It is referred to as disk00. Disk00 is not guaranteed to be the system drive or the 'key' CDS network file system (CDNFS) drive. For example, the system drives on a 2S6 are internal (disk24 and disk25), and the 'key' CDNFS disk is typically disk00, although it can move to other disks as a result of a missing or bad 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 VDS-OS system on the SE runs at a degraded state. On a generic UCS system the boot partition resides on the system disk (single disk, no RAID). In the event that this disk dies, the system is unbootable. If one of the critical disk drives goes bad at run time, the VDS-OS system applications can malfunction, hang, or crash, or the VDS-OS system can hang or crash. Monitor the critical disk drives on an SE and report any disk drive errors to Cisco Technical Assistance Center (TAC).

In a RAIDed system, if a single system disk fails, the system handles the failure seamlessly (apart from any would be CDNFS partitions). If the 'key' CDNFS disk, typically the lowest numbered disk containing CDNFS, fails the system enters an bad state and must be rebooted. In a non-RAID system, if the system disk fails, the system is no longer boots.

With a VDS-OS system, a disk device error is defined as any of the following events:

- Small Computer Systems Interface (SCSI) or Integrated Drive Electronics (IDE) device error is printed by a Linux kernel.
- Disk device access by an application (for example, an open(2), read(2), or write(2) system call) fails with an EIO error code.
- 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 Simple Network Management Protocol (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.

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 VDS-OS system automatically reboots the SE. For more information about specifying this threshold, see the "Specifying the Disk Error-Handling Threshold" section on page 2-91.

You can remap bad (but unused) sectors on a SCSI drive and Serial Advanced Technology Attachment (SATA) drives using the **disk repair** command.

Disk Latent Sector Error Handling

Latent Sector Errors (LSE) are when a particular disk sector cannot be read from or written to, or when there is an uncorrectable ECC error. Any data previously stored in the sector is lost. There is also a high probability that sectors in close proximity to the known bad sector have as yet undetected errors, and therefore are included in the repair process.

The syslog file shows the following disk I/O error message and smartd error message when there are disk sector errors:

Apr 28 21:00:26 U11-CDE220-2 kernel: %SE-SYS-4-900000: end_request: I/O error, dev sdd, sector 4660

Apr 28 21:00:26 U11-CDE220-2 kernel: %SE-SYS-3-900000: Buffer I/O error on device sdd, logical block 582

Apr 28 21:04:54 U11-CDE220-2 smartd[7396]: %SE-UNKNOWN-6-899999: Device: /dev/sdd, SMART Prefailure Attribute: 1 Raw_Read_Error_Rate changed from 75 to 73

Apr 28 21:04:54 U11-CDE220-2 smartd[7396]: %SE-UNKNOWN-6-899999: Device: /dev/sdd, SMART Usage Attribute: 187 Reported_Uncorrect changed from 99 to 97

Apr 28 21:04:54 U11-CDE220-2 smartd[7396]: %SE-UNKNOWN-2-899999: Device: /dev/sdd, ATA error count increased from 1 to 3

Specifying the Disk Error-Handling Threshold

You can configure a disk error-handling threshold to determine how many disk errors or bad sectors can be detected before the disk drive is automatically marked as bad.

The **disk error-handling threshold bad-sectors** command determines how many bad sectors can be detected before the disk drive is automatically marked as bad. By default, this threshold is set to 15. To change the default threshold, use the **disk error-handling threshold bad-sectors** 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 VDS-OS 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.

The **disk error-handling threshold errors** command determines how many disk errors can be detected before the disk drive is automatically marked as bad. By default, this threshold is set to 500. To change the default threshold, use the **disk error-handling threshold errors** command. Specify 0 if you never want the disk drive to be marked as bad.

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

Examples

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

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

Related Commands

Command	Description
disk (EXEC mode)	Allocates the disks among the CDNFS and sysfs file systems.
show disk	Displays the disk configurations.
show disk details	Displays currently effective configurations with more details.

dnslookup

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

dnslookup *line*

Syntax Description

line	Domain name of host on the network.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **dnslookup** command accepts IPv6 address. If an IPv6 address is specified in the dnslookup command, the server replies to a query including the IPv6 address and the IPv6 address displays in the output of the and **tcpdump** and **netstat** commands and all logs.

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 (EXEC configuration)

To access privileged commands in EXEC configuration modes, use the **enable** command in EXEC configuration mode.

enable

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

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

Examples

The following example shows how to access privileged EXEC configuration mode:

```
ServiceEngine> enable
ServiceEngine#
```

Related Commands

Command	Description
disable	Turns off the privileged EXEC commands.
exit	Exits from interface, global configuration, or privileged EXEC configuration modes.

enable (global configuration)

To modify enable password parameters, use the **enable password** command in global configuration mode.

enable password {0 | 1 | *word*}

Syntax Description

password	Assigns a privileged-level password.
0	Specifies an unencrypted password will follow.
1	Specifies a hidden password will follow.
word	The unencrypted (cleartext) user password.

Defaults

None

Command Modes

Global configuration mode.

Examples

The following example shows how to assign a privileged-level unencrypted password:

```
ServiceEngine> enable password 0 xxxx
ServiceEngine#
```

end

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

end

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

Use the **end** command to exit global configuration mode after completing any changes to the running configuration. To save new configurations to nonvolatile random-access memory (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

Command	Description
exit	Exits from interface, global configuration, or privileged EXEC configuration modes.

exec-timeout

To configure the length of time that an inactive Telnet or Secure Shell (SSH) session remains open, use the **exec-timeout** command in global configuration mode. 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. The range is from 0–44640. The default is 15.

Defaults

The default is 15 minutes.

Command Modes

Global configuration (config) mode.

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 shows how to configure 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

Command	Description
sshd	Configures the SSH service parameters.
telnet enable	Enables the Telnet services.

exit

To access commands in EXEC configuration mode 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

None

Command Modes

EXEC, global configuration (config), and interface configuration (config-if) modes.

Usage Guidelines

Use the **exit** command in any configuration mode to return to EXEC configuration 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 shows how to exit the global configuration mode and return to the privileged-level EXEC configuration mode:

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

The following example shows how to exit the privileged-level EXEC configuration mode and return to the user-level EXEC configuration mode:

```
ServiceEngine# exit
ServiceEngine>
```

Related Commands

Command	Description
end	Exits configuration and privileged EXEC configuration modes.

expert-mode

To configure debugshell, use the **expert-mode** command in global configuration mode.

expert-mode password [**encrypted**] *password*

Syntax Description

password	Sets the expert mode password.
encrypted	(Optional) Encrypts the password.
password	The encrypted password.

Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

This is a customer configurable password for allowing to enter engineering mode for troubleshooting purposes. The function prompts the user for the current admin password to verify that the user attempting to set the expert-mode password is authorized to do so. If the user is authenticated, the user is prompted twice to enter the new expert-mode password. The new expert-mode password is encrypted prior to being persisted.

Examples

The following example shows how to configure debugshell:

```
ServiceEngine(config)# expert-mode password encrypted xxxx
New Expert Mode Password: xxxx
Confirm New Expert Mode Password: xxxx
Password successfully changed
```

external-ip

To configure up to eight external Network Address Translation (NAT) IP addresses, use the **external-ip** command in global configuration mode. 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

None

Command Modes

Global configuration (config) mode.

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 Real-Time Streaming Protocol (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 a VDS-OS network, there are two methods for a device registered with the VOSM (SEs, SRs, or the standby VOSM) to obtain configuration information from the primary VOSM. The primary method is for the device to periodically poll the primary VOSM on port 443 to request a configuration update. You cannot configure this port number. The backup method is when the VOSM 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. VDS-OS networks do not work reliably if devices registered with the VOSM are unable to poll the VOSM 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 VOSMs) 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 VOSM. 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 VOSM 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 VOSM's inside local IP address on its NAT, and using this address, rather than the VOSM's inside local IP address in the **VOSM ip** *ip_address* command when you register the device to the VOSM. If an SE or SR is inside a NAT and the VOSM 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 shows how to configure 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
```

find-pattern

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

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

None

Command Modes

EXEC configuration mode.

Usage Guidelines

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

Examples

The following example shows how to search 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

Command	Description
cd	Changes the directory.
dir	Displays the list of files in a directory.
lls	Displays the files in a long list format.
ls	Lists the files and subdirectories in a directory.

ftp

To enable File Transfer Protocol (FTP) services, use the **ftp** command in global configuration mode. To cancel the request, use the **no** form of this command.

ftp enable

no ftp enable

Syntax Description

enable	Enables FTP services.

Defaults

None

Command Modes

Global configuration (config) mode.

Examples

The following example shows how to enable FTP services:

```
ServiceRouter# ftp enable
```

Related Commands

Command	Description
show ftp	Displays the caching configuration of the FTP.

gulp

To capture lossless gigabit packets and write them to disk, use the **gulp** command in EXEC configuration mode.

gulp *line*

Syntax Description

line	(Optional) Specifies gulp options, enter **-h** to get help.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **gulp** utility captures lossless gigabit packets and writes them to disk, as well as captures packets remotely. The **gulp** utility has the ability to read directly from the network.

To view the list of options, enter **gulp --h**.

```
ServiceEngine# gulp --help

Usage: /ruby/bin/gulp [--help | options]
    --help      prints this usage summary
    supported options include:
      -d        decapsulate Cisco ERSPAN GRE packets (sets -f value)
      -f "..."  specify a pcap filter - see manpage and -d
      -i eth#|- specify ethernet capture interface or '-' for stdin
      -s #      specify packet capture "snapshot" length limit
      -r #      specify ring buffer size in megabytes (1-1024)
      -c        just buffer stdin to stdout (works with arbitrary data)
      -x        request exclusive lock (to be the only instance running)
      -X        run even when locking would forbid it
      -v        print program version and exit
      -Vx...x   display packet loss and buffer use - see manpage
      -p #      specify full/empty polling interval in microseconds
      -q        suppress buffer full warnings
      -z #      specify write blocksize (power of 2, default 65536) for long-term capture
      -o dir    redirect pcap output to a collection of files in dir
      -C #      limit each pcap file in -o dir to # times the (-r #) size
      -W #      overwrite pcap files in -o dir rather than start #+1
      -B        check if select(2) would ever have blocked on write
      -Y        avoid writes which would block
```

Table 2-4 lists the gulp options and provides a description of each.

Table 2-4 gulp Options

Option	Description
-d	Decapsulates packets from a Cisco Encapsulated Remote SPAN Port (ERSPAN). Sets the pcap filter expression to "proto gre" and strips off Cisco generic routing encapsulation (GRE) headers (50 bytes) from the packets captured. (If used with -f option note that arguments are processed left to right).
-f	Specify a pcap filter expression. This may be useful to select one from many GRE streams if using -d, or if not using -d, because filtering out packets in the kernel is more efficient than passing them first through the **gulp** utility and then filtering them out.
-i *eth#*	Specify the network interface to read from. The default is eth1 or the value of the environment variable $CAP_IFACE, if present. Specifying a hyphen (-) as the interface reads a pcap file from the standard input instead. (If you forget the -d option during a live capture, you can decapsulate offline this way.)
-r #	Specify a ring buffer size (in megabytes). Values from 1–1024 are permitted. The default is 100. If possible, the ring buffer is locked into RAM.
-c	Copy and buffer bytes from stdin to stdout—do not read packets from the network and do not assume anything about the format of the data. This may be useful to improve the real-time performance of another application.
-s #	Specify packet capture snapshot length. By default, complete packets are captured. For efficiency, captured packets can be truncated to a given length during the capture process, which reduces capture overhead and pcap file sizes. (If used with the -d option, it specifies the length after decapsulation.)
-x	Use file locking to request (by way of exclusive lock) that this is the only instance of the **gulp** utility running. If other instances are already running, they must be stopped before the **gulp** utility can start with this option.
-X	Override an exclusive lock (-x option) and run anyway. An instance of **gulp** started this way holds a shared lock if no exclusive locks were broken; otherwise, it holds no locks at all (causing a subsequent attempt to get an exclusive lock to succeed).
-v	Print program version and exit.
-V xxxxxxxx	If the string of Xs is wide enough (10 or more), it is overwritten twice per second with a brief capture status update consisting of one digit followed by two percentages. The digit is the number of decimal digits in the actual count of lost packets (0 indicates no drops). The two percentages are the current and maximum ring buffer utilization. The updated argument string can be seen with the ps -x option (or equivalent). If the string of Xs is too short to hold the information above, a more verbose status line is written, twice per second, to standard error instead. The first method is probably more useful to occasionally check on long captures and the second is more convenient while experimenting and setting up a capture.
-p #	Specify the thread polling interval (in microseconds). The reader and writer threads poll at this interval when the ring buffer is full or empty. Polling (even frequently) on modern hardware consumes immeasurably few resources. The default interval is 1000.
-q	Suppress warnings about the ring buffer being full. If input is not from a live capture, no data is lost when the ring buffer fills so the warning can be safely suppressed. If stdin is actually a file, warning suppression happens automatically.
-z #	Specify output write block size. Any power of two between 4096 and 65536. The default is 65536.

Table 2-4 gulp Options (continued)

Option	Description
-o *dir*	Redirects pcap output into a collection of files in the specified directory. Pcap files are named pcap###, where ### starts at 000 and increments. The directory must exist and be writable by the user running the **gulp** utility.
-C #	When using the -o option, start a new pcap file when the old one reaches about # times the size of the ring buffer. The default value is 10 and the default ring buffer size is 100MB; so by default, pcap files grow to about 1000 MB before a new one is started. Since some programs read an entire pcap file into memory when using it, splitting the output into chunks can be helpful.
-W #	Specifies a maximum number of pcap files to create before overwriting them. The default is to never overwrite them. This option allows capturing to occur indefinitely with finite disk space.
-B	This option enables the code to check before each write whether the write would block. When the **gulp** utility exits, it announces whether any writes would have been blocked.
-Y	This option writes which ones would be blocked, but are deferred until they are not blocked.

Examples

The following example shows how to get a basic capture on eth1 with a pcap filter:

```
ServiceEngine# gulp -i eth1 -f "..." > pcapfile
```

The ellipsis (...) refers to the Berkeley Packet Filter (pcap) expressions, such as “host foo.”

The following example shows how to get a capture of the 10 most recent files of a 200 MB ring buffer to 1000 MB files:

```
ServiceEngine# gulp -i eth1 -r 200 -C 10 -W 10 -o pcapdir
```

Related Commands

Command	Description
netmon	Displays the transmit and receive activity on an interface.
netstatr	Displays the rate of change of netstat statistics.
ss	Dumps socket statistics.
tcpmon	Searches all TCP connections.

help

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

help

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration and global configuration (config) modes.

Usage Guidelines

You can get help at any point in a command by entering a question mark (**?**). If nothing matches, the help list is 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** command in EXEC configuration mode:

```
ServiceEngine# help
Help may be requested at any point in a command by entering a question mark '?'. If
nothing matches, the help list will be empty and you must backup until entering a '?'
shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a command argument (e.g. 'show ?')
and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know
what arguments match the input (e.g. 'show stat?'.)
```

hostname

To configure the device's network hostname, use the **hostname** command in global configuration mode. 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 (config) mode.

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 (-).
- Maximum length is 30 characters.
- Following characters are considered invalid 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

Command	Description
dnslookup	Resolves a host or domain name to an IP address.
ip	Configures the IP.
show hosts	Displays the IP domain name, name servers, IP addresses, and host table.

http

To configure HTTP-related parameters, use the **http** command in EXEC configuration mode.

http asx-302-redirect enable

Syntax Description

asx-302-redirect	Configures 302 response for asx requests.
enable	Enables 302 redirection for asx requests.

Defaults

None

Command Modes

EXEC configuration mode.

Examples

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

```
ServiceEngine# install VDS-OS-2.2.1.7-K9.bin
```

install

To install the VDS-OS software image, use the **install** command in EXEC configuration mode.

install *imagefile_name*

Syntax Description		
	imagefile_name	Name of the .bin file that you want to install.

Defaults

None

Command Modes

EXEC configuration mode.

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 system file system (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, VDS-OS-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 VDS-OS-2.2.1.7-K9.bin
```

Related Commands

Command	Description
copy ftp install	Installs an image file from a File Transfer Protocol (FTP) server onto a local device.
copy http install	Installs an image file from an HTTP server onto a local device.
reload	Halts a device and performs a cold restart.

interface

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

interface {**GigabitEthernet** *slot/port_num* [**autosense** | **bandwidth** {**10** | **100** | **1000**} | **channel-group** *group_interface* | **description** *line* | **full-duplex** | **half-duplex** | **ip** {**access-group** {*access_list_num* {**in** | **out**} | *name*} | **address** {*ip_address_netmask* | **range** *low_num high_num netmask*} | **ipv6** {**access-group** {*access_list_num* {**in** | **out**}| *access_list_name* {**in** | **out**}} | **address** {*range low_num high_num netmask* {*prefix* | *subnet_mask*} | *ip_addr/mask*} | **mtu** *mtu_size* | **shutdown** | **standby** *num* [**priority** *num*] | **tx-queue-limit** *queue_length*] | **PortChannel** *num* [**autosense** | **bandwidth** {**10** | **100** | **1000**} | **description** line | **full-duplex** | **half-duplex** | **ip** *line* | **ipv6** *line* | **lacp** | **shutdown** | **standby** *num* [**priority** num] | **Standby** *group_number* [**description** *line* | **errors** *error_num* | **ip address** {*ip_address_netmask* | **range** *low_num high_num netmask*}| **ipv6 address** {**range** *low_num high_num netmask* {*prefix* | *subnet_mask*} | *ip_addr/mask*} | **shutdown**] | **TenGigabitEthernet** *slot/port_num* [**autosense** | **bandwidth** {**10** | **100** | **1000**} **channel-group** *group_interface* | **description** *line* | **full-duplex** | **half-duplex** | **ip** {**access-group** {*access_list_num* {**in** | **out**} | *name*} | **address** {*ip_address_netmask* | **range** *low_num high_num netmask*} | **ipv6** {*acccess-group* {*access_list_num* {**in** | **out**}| *access_list_name* {**in** | **out**}} | **address** {**range** *low_num high_num netmask* {*prefix* | *subnet_mask*} | *ip_addr/mask*} | **mtu** *mtu_size* | **shutdown** | **standby** *num* [**priority** *num*] | **tx-queue-limit** *queue_length*]

no interface {**GigabitEthernet** *slot/port_num* [**autosense** | **bandwidth** {**10** | **100** | **1000**} | **channel-group** *group_interface* | **description** *line* | **full-duplex** | **half-duplex** | **ip** {**access-group** {*access_list_num* {**in** | **out**} | *name*} | **address** {*ip_address_netmask* | **range** *low_num high_num netmask*} | **ipv6** {**access-group** {*access_list_num* {**in** | **out**}| *access_list_name* {**in** | **out**}} | **address** {*range low_num high_num netmask* {*prefix* | *subnet_mask*} | *ip_addr/mask*} | **mtu** *mtu_size* | **shutdown** | **standby** *num* [**priority** *num*] | **tx-queue-limit** *queue_length*] | **PortChannel** *num* [**autosense** | **bandwidth** {**10** | **100** | **1000**} | **description** line | **full-duplex** | **half-duplex** | **ip** *line* | **ipv6** *line* | **lacp** | **shutdown** | **standby** *num* [**priority** num] | **Standby** *group_number* [**description** *line* | **errors** *error_num* | **ip address** {*ip_address_netmask* | **range** *low_num high_num netmask*}| **ipv6 address** {**range** *low_num high_num netmask* {*prefix* | *subnet_mask*} | *ip_addr/mask*} | **shutdown**] | **TenGigabitEthernet** *slot/port_num* [**autosense** | **bandwidth** {**10** | **100** | **1000**} **channel-group** *group_interface* | **description** *line* | **full-duplex** | **half-duplex** | **ip** {**access-group** {*access_list_num* {**in** | **out**} | *name*} | **address** {*ip_address_netmask* | **range** *low_num high_num netmask*} | **ipv6** {*access-group* {*access_list_num* {**in** | **out**}| *access_list_name* {**in** | **out**}} | **address** {**range** *low_num high_num netmask* {*prefix* | *subnet_mask*} | *ip_addr/mask*} | **mtu** *mtu_size* | **shutdown** | **standby** *num* [**priority** *num*] | **tx-queue-limit** *queue_length*]

Syntax Description

GigabitEthernet	Selects a Gigabit Ethernet interface to configure.
slot/port_num	Slot and port number for the selected interface. The slot range is from 1 to 14; the port range is from 0 to 0. The slot number and port number are separated with a forward slash character (/).
autosense	(Optional) Specifies interface autosense.
bandwidth	(Optional) Configures the interface bandwidth.
10	Specifies the interface bandwidth as 10 Mbits per second.
100	Specifies the interface bandwidth as 100 Mbits per second.

1000	Specifies the interface bandwidth as 1000 Mbits per second.
channel-group	(Optional) Configures the EtherChannel group.
group_interface	EtherChannel group to which the interface belongs. The range is 1 to 4.
description	(Optional) Specifies interface specific description.
line	Text describing this interface
full-duplex	(Optional) Specifies full-duplex.
half-duplex	(Optional) Specifies half-duplex.
ip	(Optional) Interface Internet Protocol configuration commands.
access-group	Specifies access control for packets.
access_list_num	IP access list (standard or extended).
in	Specifies inbound packets.
out	Specifies outbound packets.
name	Specifies the access-list name.
address	Sets the IP address of the interface.
ip_address	IP address of the interface
netmask	Netmask of the interface.
range	IP address range.
low_num	IP address low range of the interface.
high_num	IP address low range of the interface.
netmask	Netmask of the interface.
ipv6	(Optional) Interface IPv6 configuration commands.
access-group	Specifies access control for packets.
ip_access_list	IP access list (standard or extended).
in	Inbound packets.
out	Outbound packets.
access-list-name	Specifies an access list name.
address	Specifies the IPv6 address of the interface.
range	Specifies the IPv6 address range.
low-num	Specifies the IPv6 address low range of the interface.
high-num	Specifies the IPv6 address high range of the interface.
prefix	Interface prefix. The range is from 1 to 128.
ip_addr/netmask	IPv6 address/netmask of the interface in format X:X:X:X: :X/<0-128>.
mtu	Sets the interface Maximum Transmission Unit (MTU).
mtu_size	MTU size in bytes. The range is 576 to 9216.
shutdown	(Optional) Shuts down the specific portchannel interface.
standby	(Optional) Standby interface configuration commands.
interface_group_num	Group number for the selected interface. The range is from 1 to 4.
priority	Sets the priority of the interface. Default value is 100.
standby_group_priority	Set the priority of the interface for the standby group. The range is from 0 to 4294967295.
tx-queue-limit	Sets the interface maximum Transmission Queue Length.

queue_length	Sets the limit on the transmission queue length. The range is from 1000 to 80000.
PortChannel	Selects the Ethernet Channel of interfaces to be configured.
num	Sets the Ethernet Channel interface number. The range is from 1 to 4.
lacp	Specifies Link Aggregation Control Protocol.
Standby	Specifies a standby group number.
standby_group_num	Standby group number. The range is from 1 to 4.
description	(Optional) Standby interface description.
line	Text describing this interface.
errors	Sets the maximum number of errors allowed on this interface.
error_num	Maximum number of errors allowed on this interface for the standby group. The range is from 1 to 2147483647.
ip	Sets the IP address of the standby group.
address	Sets the IP address of the interface.
standby_group_ip_addr	IP address of the standby group.
standby_group_ netmask	Netmask of the standby group.
range	Sets the IP address range of the standby group.
low_range	IP address low range of an interface.
high_range	IP address high range of an interface.
interface_netmask	Netmask of the interface.
TenGigabitEthernet	Selects a ten Gigabit Ethernet interface to configure.

Defaults

Standby priority: 100.

Command Modes

Global configuration (config) mode.

Usage Guidelines

Note The Gigabit Ethernet interfaces are shared between CIMC and UCS for UCS devices (specifically UCS220). The default values for duplex, speed, auto negotiation and advertising *cannot* be changed.

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

EtherChannel for VDS-OS 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 current link status of each interface.

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.

Configuring Multiple IP Addresses

The Multiple Logical IP Addresses feature supports up to 24 unique IP addresses within the same subnet for the same interface.

When you configure multiple IP addresses on an SE using either the range option or using individual commands, the **show running-config** output displays all the IP addresses individually. The netmask value is unique for each interface, so under a single interface you cannot have multiple IP addresses with different netmask values.

Configuring IPv6

When configuring an IPv6 address on the interface, if <*ipv6addr*> is specified, it must be in the form of hexadecimal using16-bit values between colons (X:X:X:X: :X). Optionally, a double colon may be used when consecutive 16-bit values are denoted as zero.

To configure the IPv6 access list on an interface, first configure the Access List using the **access-list enable** command; **<in | out>** means apply for inbound or outbound packets.

```
interface {<GigabitEthernet | Portchannel | Standby | TenGigabitEthernet>} ipv6
access-group <access_ list_number | access_list_name> <in | out>
```

Examples

The following example shows how to create 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 how to remove 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** command in EXEC configuration mode:

```
ServiceEngine# show running-config
.
.
.
interface GigabitEthernet 0/0
description This is an interface to the WAN
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
```

The following example shows how to configure multiple IP addresses using a range command:

```
ServiceEngine(config)# interface PortChannel 2
ServiceEngine(config-if)# ip address range 2.2.2.3 2.2.2.6 255.255.255.0
```

The following example shows a sample output of the **show running-config** command in EXEC configuration mode after configuring multiple IP addresses:

```
ServiceEngine# show running-config
.
interface PortChannel 4
 ip address 2.2.2.3 255.255.255.0
 ip address 2.2.2.4 255.255.255.0
 ip address 2.2.2.5 255.255.255.0
 ip address 2.2.2.6 255.255.255.0
 exit
```

Related Commands

Command	Description
show interface	Displays the hardware interface information.
show running-config	Displays the current operating configuration.
show startup-config	Displays the startup configuration.

iostat

To Show CPU and I/O statistics for devices and partitions, use the **iostat** command in EXEC configuration mode.

iostat [*line*]

Syntax Description

line	Specifies iostat options.

Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to display CPU statistics:

```
ServiceEngine# iostat
Linux 2.6.32.52-cds-64 (W14-UCS220-2)   10/16/12        _x86_64_        (32 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           0.00    0.03    0.03    0.00    0.00   99.93

Device:            tps    kB_read/s    kB_wrtn/s    kB_read    kB_wrtn
sdc               1.79         7.24        30.89     580715    2478770
sdd               0.00         0.05         0.03       4143       2057

ServiceEngine#
```

ip (global configuration)

To change initial network device configuration settings, use the **ip** command in global configuration mode. To delete or disable these settings, use the **no** form of this command.

ip {**access-list** (see "ip access-list" section on page 127) | **default-gateway** *ip_address* [*gateway_ip_addr*] | **domain-name** *name1 name2 name3* | **name-server** *ip_addresses* | **path-mtu-discovery enable** | **route** *dest_IP_addr dest_netmask default_gateway* [**interface** *source_IP_addr*]}

no ip {**access-list** | **default-gateway** *ip_address* [*gateway_ip_addr*] | **domain-name** *name1 name2 name3* | **name-server** *ip_addresses* | **path-mtu-discovery enable** | **route** *dest_IP_addr dest_netmask default_gateway* [**interface** *source_IP_addr*]}

Syntax Description

access-list	Specifies the access list.
default-gateway	Specifies the default gateway (if not routing IP).
ip_address	IP address of the default gateway.
gateway_ip_addr	(Optional) Gateway IP address (maximum of 14).
domain-name	Specifies domain names.
name1 through *name3*	Domain name (up to three can be specified).
name-server	Specifies the address of the name server.
ip_addresses	IP addresses of the domain server (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_IP_addr	Destination route address.
dest_netmask	Netmask address.
default_gateway	Gateway address.
interface	Configures source policy routing to route outgoing traffic using the same interface where the request was received.
source_IP_addr	IP address of the interface configured for source policy routing.

Defaults

None

Command Modes

Global configuration (config) mode.

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 Domain Name System (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 VDS-OS 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 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 started by the sending device. If a server does not support IP Path MTU Discovery, the receiving device has 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.

Source Policy Routes

To configure source policy routing, use the **ip route** command with the interface option. By using source policy routing, the reply packet to a client leaves the SE on the same interface where the request came in. Source policy routing tables are automatically instantiated based on the interface subnets defined on the system. The policy routes are added automatically to the policy routing tables based on the nexthop gateway of the routes in the main routing table.

When configuring multiple IP address you must configure a default gateway in the same subnet. You can configure multiple gateways (up to 14).

The CDE220-2S3i supports multiple IP addresses, which includes specifying the default gateway and IP routes. The IP routes, source policy routes, were added to ensure incoming traffic would go out the same interface it came in on. An IP route was added using the **interface** keyword and has the following syntax:

ip route <*dest_IP_addr*> <*dest_netmask*> <*default_gateway*> *interface* <*source_IP_addr*>

In the following example, all destination traffic (IP address of 0.0.0.0 and netmask of 0.0.0.0) sent from the source interface, 8.1.0.2, uses the default gateway, 8.1.0.1. This is a default policy route.

ip route 0.0.0.0 0.0.0.0 8.1.0.1 interface 8.1.0.2

A non-default policy route defines a specific destination (IP address and netmask). The following **ip route** command is an example of a non-default policy route:

ip route 10.1.1.0 255.255.255.0 <*gateway*> interface <*source_IP_addr*>

Because you had to define the default gateway for all the interfaces as part of the multi-port support feature, the equivalent source policy route is automatically generated in the routing table. The following example shows the output for the **show ip route** command after upgrading the software with the default source policy routes highlighted in bold and the non-default policy routes highlighted in italics:

```
ServiceEngine# show ip route

Destination      Gateway          Netmask
---------------- ---------------- ----------------
172.22.28.0      8.1.0.1          255.255.255.128
6.21.1.0         0.0.0.0          255.255.255.0
8.2.1.0          0.0.0.0          255.255.255.0
8.2.2.0          0.0.0.0          255.255.255.0
171.70.77.0      8.1.0.1          255.255.255.0
8.1.0.0          0.0.0.0          255.255.0.0
0.0.0.0          8.1.0.1          0.0.0.0
0.0.0.0          8.2.1.1          0.0.0.0
0.0.0.0          8.2.2.1          0.0.0.0

Source policy routing table for interface 8.1.0.0/16
172.22.28.0      8.1.0.1          255.255.255.128
171.70.77.0      8.1.0.1          255.255.255.0
8.1.0.0          0.0.0.0          255.255.0.0
0.0.0.0          8.1.0.1          0.0.0.0

Source policy routing table for interface 8.2.1.0/24
8.2.1.0          0.0.0.0          255.255.255.0
0.0.0.0          8.2.1.1          0.0.0.0

Source policy routing table for interface 8.2.2.0/24
8.2.2.0          0.0.0.0          255.255.255.0
0.0.0.0          8.2.2.1          0.0.0.0
```

If you have a default source policy route where the gateway is not defined as a default gateway, then you must add it after upgrading the software. For example, if you had a source policy route with a gateway of 6.23.1.1 for a source interface of 6.23.1.12, and you did not specify the gateway as one of the default gateways, you would need to add it.

If you have a non-default source policy route, then you must add it as a regular static route (without the obsoleted interface keyword) after upgrading the software. This route is then added to the main routing table as well as the policy routing table.

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.

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 VDS-OS 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. 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.

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 Type of Service (ToS) octet (RFC 791) and the IPv6 traffic class octet. 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 Per-Hop Behavior (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).

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:

- 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.

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 are dropped according to the following guideline:

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

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

In the following example, packets in the AF13 class are dropped before packets in the AF12 class, which in turn are 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.

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 VDS-OS 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.

Examples

The following example shows how to configure 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 shows how to configure 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 shows how to configure 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 shows how to configure 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
```

The following example shows how to configure source policy routing for the SE interface assigned with the IP address 192.168.1.5:

```
ServiceEngine(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1 interface 192.168.1.5
```

Related Commands

Command	Description
ip (interface configuration)	Configures the interface Internet Protocol.
show ip routes	Displays the IP routing table.

ip (interface configuration)

To configure the interface Internet Protocol, use the **interface** command in interface configuration mode. To delete or disable these settings, use the **no** form of this command.

ip {**access-group** {*num* {**in** | **out**} {*name* {**in** | **out**} | **address** {*ip_addr netmask* | **range** {*ip_addr_low ip_addr_high netmask*}}

no ip {**access-group** {*num* {**in** | **out**} {*name* {**in** | **out**} | **address** {*ip_addr netmask* | **range** {*ip_addr_low ip_addr_high netmask*}}

Syntax Description

access-group	Specifies access control for incoming or outgoing packets.
num	Specifies an IP access list by number, in standard or extended form. The range is from 1-199.
in	Configures the IP access list that apply to inbound packets.
out	Configures the IP access list that apply to outbound packets.
name	Name of the access list.
in	Configures the access list name inbound packets.
out	Configures the access list name outbound packets.
address	Set the IP address of an interface.
ip-addr	IP address of the interface.
netmask	Netmask of the interface.
range	Specifies the IP address range.
ip_addr_low	IP address low range of an interface.
ip_addr_high	IP address high range of an interface.
netmask	Netmask of the interface.

Defaults

None

Command Modes

Interface configuration (config-if) mode.

Usage Guidelines

You can configure multiple IP addresses for Gigabit Ethernet, port channel and Standby interfaces in the SEs. With multiple IP support, the SEs can stream the content under a specific IP while having another stream with different source IP address under the same interface.

The **ip** command configures up to 24 unique IP addresses within the same subnet for the same Gigabit Ethernet, port channel and Standby interface. You can add and delete IP addresses for each interface without affecting other configured IP addresses.

Note All IP addresses configured in the same interface must be in the same subnet.

The **ip range** command adds and deletes an IP address range per interface without affecting other configured IP addresses, and it notifies the SR and VOSM on the added and deleted IP address. The IP address can only be deleted when it is already disassociated from the delivery service. If the delivery service's IP address has been updated, for example from 10.1.1.1 to 10.1.1.5, the service is not interrupted. The new stream uses the new IP address.

Examples

Configuring an IP Address Range

The following example shows how to configure an IP address in a range:

```
ServiceEngine(config)# interface PortChannel 1
ServiceEngine(config-if)# ip address 2.2.2.2 255.255.255.0
ServiceEngine(config-if)# ip address range 2.2.2.3 2.2.2.10 255.255.255.0
ServiceEngine(config-if)# ip address range 2.2.2.12 2.2.2.20 255.255.255.0
```

If the user configures an IP address range but one or more of the IP addresses in the range matched with an already configured IP address, the configuration is still accepted. For example, if interface PortChannel 1 has the following configuration:

```
interface PortChannel 1
ip address 2.2.2.2 255.255.255.0
ip address 2.2.2.3 255.255.255.0
ip address 2.2.2.5 255.255.255.0
ip address 2.2.2.12 255.255.255.0
```

The following configuration is accepted and the IP address in the range (not the same subnet) is rejected:

```
ServiceEngine# configure terminal
ServiceEngine(config)# interface PortChannel 1
ServiceEngine(config-if)# ip address range 2.2.2.3 2.2.2.4 255.255.255.0
ServiceEngine(config-if)# end
```

If the interface PortChannel 1 has the following configuration:

```
interface PortChannel 1
ip address 2.2.2.2 255.255.255.0
ip address 2.2.2.5 255.255.255.0
ip address 2.2.2.12 255.255.255.0
```

And you enter the following commands:

```
ServiceEngine# configure terminal
ServiceEngine(config)# interface PortChannel 1
ServiceEngine(config-if)# ip address range 2.2.3.9 2.2.3.15 255.255.255.0
ServiceEngine(config-if)# end
```

It is an invalid IP address range and an incompatible netmask.

Configuring an IP Address

The following example shows how to configure an individual IP address:

```
ServiceEngine(config)# interface PortChannel 1
ServiceEngine(config-if)# ip address 2.2.2.2 255.255.255.0
ServiceEngine(config-if)# ip address 2.2.2.3 255.255.255.0
ServiceEngine(config-if)# ip address 2.2.2.10 255.255.255.0
```

Removing an IP Address

The following example shows how to remove an IP address range configuration:

```
ServiceEngine(config)# interface PortChannel 1
```

```
ServiceEngine(config-if)# no ip address range 2.2.2.3 2.2.2.10 255.255.255.0
```

The following example shows how to remove an IP address configuration:

```
ServiceEngine(config)# interface PortChannel 1
ServiceEngine(config-if)# no ip address 2.2.2.3 255.255.255.
```

Related Commands

Command	Description
interface (global configuration)	Configures a Gigabit Ethernet or port channel interface.
show interface	Displays the hardware interface information.
show running-config	Displays the current operating configuration.

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** command in global configuration modes. To remove access control lists, use the **no** form of this command.

ip access-list {**extended** {*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*}}] | *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** {*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_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*}}] | *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** {*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. The range is from 1 to 500.
deny	(Optional) Causes packets that match the specified conditions to be dropped.

num	IP Protocol Number.
ip address	Source IP address.
any	Any source host.
host	A single host address.
gre	Specifies generic routing encapsulation (GRE) Tunneling by Cisco.
icmp	Specifies Internet Control Message Protocol.
ip	Specifies Any IP Protocol.
tcp	Specifies Transport Control Protocol.
udp	Specifies 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 (config) mode.

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 Internet Control Message Protocol (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 2-7. For a list of supported UDP and TCP keywords, see Table 2-5 and Table 2-6.

Use access lists to control access to specific applications or interfaces on an SE. An ACL consists of one or more condition entries that specify the kind of packets that the SE drops or accepts 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:

- 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.
- SE is deployed anywhere within the enterprise. As with routers and switches, the administrator wants to limit Telnet and SSH access to the IT source subnets.
- 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 and SSH access to the SE.
- SE is deployed as a reverse proxy in an untrusted environment. The SE administrator wants 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. Use a standard access list for providing access to the Simple Network Management Protocol (SNMP) server or to the Trivial File Transfer Protocol (TFTP) gateway or 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 2-5 lists the UDP keywords that you can use with extended access lists.

Table 2-5 UDP Keywords and Port Numbers

CLI Keyword	Description	UDP Port Number
bootpc	BOOTP client service	68
bootps	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 2-6 lists the TCP keywords that you can use with extended access lists.

Table 2-6 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	File Transfer Protocol (FTP) data connections (used infrequently)	20
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 2-7 lists the keywords that you can use to match specific ICMP message types and codes.

Table 2-7 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 one (ICMP) and the type field in the ICMP header set to three (Host Unreachable). This is the most common response. Large numbers of this datagram type on the network are indicative of network difficulties or 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.

Table 2-7 Keywords for ICMP Message Type and Code (continued)

Field	Description
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.
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 DF bit (do not fragment) 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 one (ICMP) and the type field in the ICMP header set to five (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 one (ICMP) and the type field in the ICMP header set to four (Source Quench). This datagram may be used in network management to provide congestion control. A source quench packet is issued when a router is beginning to lose packets because of 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.

Table 2-7 Keywords for ICMP Message Type and Code (continued)

Field	Description
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.
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 allow only 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

Command	Description
clear ip access-list counters	Clears the IP access list statistical information.
show ip access-list	Displays the access lists that are defined and applied to specific interfaces or applications.

ipv6

To specify the default gateway's IPv6 address, use the **ipv6** command in global configuration mode. To disable the IPv6 address, use the **no** form of this command.

ipv6 {**access-list** {**extended** {*extended_acess_list_num* [**delete** *num* | **deny** {*protocol_num* {**any** | **host** | *ipv6_addr*} | **gre** {**any** | **host** | *ipv6_addr*} | **icmpv6** {**any** | **host** | *ipv6_addr*} | **ip** {**any** | **host** | *ipv6_addr*} | **tcp** {**any** | **host** | *ipv6_addr*} | **udp** {**any** | **host** | *ipv6_addr*} | **insert** *position_num* {**deny** {*protocol_num* {**any** | **host** | *ipv6_addr*} | **gre** {**any** | **host** | *ipv6_addr*} | **icmpv6** {**any** | **host** | *ipv6_addr*} | **ip** {**any** | **host** | *ipv6_addr*} | **tcp** {**any** | **host** | *ipv6_addr*} | **udp** {**any** | **host** | *ipv6_addr*}} | **permit** {**any** | **host** | *ipv6_addr*}} | **list** [*position_start position_end*] | **move** {*move_from move_to*} | **permit** {*protocol_num* {**any** | **host** | *ipv6_addr*} | **gre** {**any** | **host** | *ipv6_addr*} | **icmpv6** {**any** | **host** | *ipv6_addr*} | **ip** {**any** | **host** | *ipv6_addr*} | **tcp** {**any** | **host** | *ipv6_addr*} | **udp** {**any** | **host** | *ipv6_addr*}}] | *access_list name* [**delete** *num* | **deny** {*protocol_num* {**any** | **host** | *ipv6_addr*} | **gre** {**any** | **host** | *ipv6_addr*} | **icmpv6** {**any** | **host** | *ipv6_addr*} | **ip** {**any** | **host** | *ipv6_addr*} | **tcp** {**any** | **host** | *ipv6_addr*} | **udp** {**any** | **host** | *ipv6_addr*}} | **insert** *position_num* {**deny** {*protocol_num* {**any** | **host** | *ipv6_addr*} | **gre** {**any** | **host** | *ipv6_addr*} | **icmpv6** {**any** | **host** | *ipv6_addr*} | **ip** {**any** | **host** | *ipv6_addr*} | **tcp** {**any** | **host** | *ipv6_addr*} | **udp** {**any** | **host** | *ipv6_addr*}} | **permit**} | **list** [*position_start position_end*] | **move** {*move_from move_to*} | **permit** {*protocol_num* {**any** | **host** | *ipv6_addr*} | **gre** {**any** | **host** | *ipv6_addr*} | **icmpv6** {**any** | **host** | *ipv6_addr*} | **ip** {**any** | **host** | *ipv6_addr*} | **tcp** {**any** | **host** | *ipv6_addr*} | **udp** {**any** | **host** | *ipv6_addr*}}]} | **standard** {*standard_acess_list_num* [**delete** *num* | **deny** {**any** | **host** | *ipv6_addr*} | **insert** *position_num* {**deny** {**any** | **host** | *ipv6_addr*} | **permit** {**any** | **host** | *ipv6_addr*}} | **list** [*position_start position_end*] | **move** {*move_from move_to*} | **permit** {**any** | **host** | *ipv6_addr*} | **default-gateway** *ip_address* | **route** *dest_ip_adder gateway_ip_addr*}

no ipv6 {**access-list** {**extended** {*extended_acess_list_num* [**delete** *num* | **deny** {*protocol_num* {**any** | **host** | *ipv6_addr*} | **gre** {**any** | **host** | *ipv6_addr*} | **icmpv6** {**any** | **host** | *ipv6_addr*} | **ip** {**any** | **host** | *ipv6_addr*} | **tcp** {**any** | **host** | *ipv6_addr*} | **udp** {**any** | **host** | *ipv6_addr*} | **insert** *position_num* {**deny** {*protocol_num* {**any** | **host** | *ipv6_addr*} | **gre** {**any** | **host** | *ipv6_addr*} | **icmpv6** {**any** | **host** | *ipv6_addr*} | **ip** {**any** | **host** | *ipv6_addr*} | **tcp** {**any** | **host** | *ipv6_addr*} | **udp** {**any** | **host** | *ipv6_addr*}} | **permit** {**any** | **host** | *ipv6_addr*}} | **list** [*position_start position_end*] | **move** {*move_from move_to*} | **permit** {*protocol_num* {**any** | **host** | *ipv6_addr*} | **gre** {**any** | **host** | *ipv6_addr*} | **icmpv6** {**any** | **host** | *ipv6_addr*} | **ip** {**any** | **host** | *ipv6_addr*} | **tcp** {**any** | **host** | *ipv6_addr*} | **udp** {**any** | **host** | *ipv6_addr*}}] | *access_list name* [**delete** *num* | **deny** {*protocol_num* {**any** | **host** | *ipv6_addr*} | **gre** {**any** | **host** | *ipv6_addr*} | **icmpv6** {**any** | **host** | *ipv6_addr*} | **ip** {**any** | **host** | *ipv6_addr*} | **tcp** {**any** | **host** | *ipv6_addr*} | **udp** {**any** | **host** | *ipv6_addr*}} | **insert** *position_num* {**deny** {*protocol_num* {**any** | **host** | *ipv6_addr*} | **gre** {**any** | **host** | *ipv6_addr*} | **icmpv6** {**any** | **host** | *ipv6_addr*} | **ip** {**any** | **host** | *ipv6_addr*} | **tcp** {**any** | **host** | *ipv6_addr*} | **udp** {**any** | **host** | *ipv6_addr*}} | **permit**} | **list** [*position_start position_end*] | **move** {*move_from move_to*} | **permit** {*protocol_num* {**any** | **host** | *ipv6_addr*} | **gre** {**any** | **host** | *ipv6_addr*} | **icmpv6** {**any** | **host** | *ipv6_addr*} | **ip** {**any** | **host** | *ipv6_addr*} | **tcp** {**any** | **host** | *ipv6_addr*} | **udp** {**any** | **host** | *ipv6_addr*}}]} | **standard** {*standard_acess_list_num* [**delete** *num* | **deny** {**any** | **host** | *ipv6_addr*} | **insert** *position_num* {**deny** {**any** | **host** | *ipv6_addr*} | **permit** {**any** | **host** | *ipv6_addr*}} | **list** [*position_start position_end*] | **move** {*move_from move_to*} | **permit** {**any** | **host** | *ipv6_addr*} | **default-gateway** *ip_address* | **route** *dest_ip_adder gateway_ip_addr*}

Syntax Description

default-gateway	Specifies the default gateway's IPv6 address.
ip_address	IPv6 address of the default gateway.

access-list	Named access-list.
route	Specifies IPv6 net route.
extended	Specifies extended IPv6 Access List.
extended_access_list_num	Extended IPv6 access-list number. The range is from 100 to199.
extended_access_list_name	Extended IPv6 Access-list name (maximum 30 characters).
delete	(Optional) Deletes a condition.
num	Position of condition to delete. The range is from 1 to 500.
deny	(Optional) Specifies packets to reject.
protocol_num	An IP Protocol Number. The range is from 1 to 255.
any	Any source or destination host.
host	A single host address.
ipv6_addr	Source or Destination IPv6 address, in format X:X:X:X: :X/(0-128).
gre	Cisco's generic routing encapsulation (GRE) Tunneling.
icmpv6	Internet Control Message Protocol.
ip	Any IP Protocol.
tcp	Transport Control Protocol.
udp	User Datagram Protocol.
insert	(Optional) Inserts a condition.
position_num	Position to insert new condition. The range is from 1 to 500.
eq	Matches only packets on a given port number.
gt	Matches only packet with a greater port number.
host	A single host address.
lt	Matches only packets with a lower port number.
neq	Matches only packets not on a given port.
range	Matches only packets in the range of port numbers.
list	(Optional) Lists conditions.
position_start	(Optional) Position of condition to start listing. The range is from 1 to 500.
position_end	(Optional) Position of condition to end listing. The range is from 1 to 500.
move	(Optional) Moves a condition.
move_from	(Optional) Position to move condition from. The range is from 1 to 500.
move_to	(Optional) Position to move condition to. The range is from 1 to 500.
permit	(Optional) Specifies packets to accept.
standard	Specifies Standard IPv6 Access List.
standard_access_list_num	Standard IPv6 access-list number. The range is from 100 to 199.
standard_access_list_name	Standard IPv6 Access-list name (maximum 30 characters).
default-gateway	Defines the default gateway's IPv6 address.
ip_address	Default gateway IPv6 address (maximum of 14), in format X:X:X.
route	Specifies the IPv6 net route.
dest_ip_adder	Destination IPv6 address, in format X:X:X:X: :X/<0-128.
gateway_ip_addr	Gateway IPv6 address, in format X:X:X:X: :X.

Defaults None

Command Modes Global configuration (config) mode.

Usage Guidelines Explosive growth in network device diversity and mobile communications, along with global adoption of networking technologies have resulted in IPv4 addresses getting exhausted. IPv4 address space has a theoretical limit of 4.3 billion addresses. IPv6 quadruples the number of network address bits from 32 bits (in IPv4) to 128 bits. This provides more than enough globally unique IP addresses for every networked device in use.

VOS-IS IPv6 ACL, a permit or deny policy for IPv6 traffic you want to filter is based on source and destination IPv6 address, plus other IPv6 protocol factors such as TCP/UDP, Internet Control Message Protocol v6 (ICMPv6) and GRE, or specify the port number. This command mirrors IPv4:

```
[no] ipv6 access-list {<standard|extended>} {<name|number>}
{<permit|deny|delete|move|insert|list>} {protocol no|protocol
name}[any|host|ipv6addr/prefix] {any|host|ipv6addr/prefix}
```

IPv6 access lists are identified by user selected names. Access lists are defined by a list of “permit” and “deny” statements.

```
[no] ip name-server {<hostname|ipv6addr|ipv4addr>}
[no] ntp server {<hostname|ipv6addr|ipv4addr>}
```

These above configurations should support both IPv6 and IPv4 addresses.

Domain Name System (DNS) Configuration

The IPv6 address name server must be configured by using the **ipv6 name-server ip-address** command.

Note The Service Router acts as the authoritative DNS server, and supports IPv6 DNS extensions.

If an IPv6 address is configured on the SR for DNS, the communication between the SR and the DNS server is over the IPv6 transport. The IPv4 address of the Service Router must be configured in the DNS server, so that the Service Router can respond to both A and AAAA queries. In this case, the communication between the DNS Server and the SR is over IPv4 transport.

Service Router

Communication between the SE and SR is through the IPv4 stack, including the keep-alive message. If IPv6 is enabled, then the keep-alive message includes the IPv6 address of the SE in the keep-alive message payload. This enables the SR to resolve the SE's IPv6 address correctly.

The SR operates as a DNS Server for the requests that belong to the delivery service to which the SR is associated. The SR is provisioned to respond to A or AAAA queries for the configured Service Routing Domain Name (RFQDN). The query can be on either an IPv4 or IPv6 transport.

The SR accepts the HTTP, Real-Time Streaming Protocol (RTSP), and Real-Time Messaging Protocol (RTMP) requests and sends back the response by way of the IPv6 transport. The SR also supports the IP-based redirection, and includes the IPv6 address of the SE in the redirect URL. If the redirect URL has the SE host name, the client sends a DNS query to the SR, and the SR responds with the SE’s IPv4 address for the A query and the SE’s IPv6 address for the AAAA query.

The Coverage Zone file supports IPv6 and IPv4 addresses. The network and subnetwork addresses in the Coverage Zone file support CIDR format (IP address with a prefix).

Examples

The following example shows how to configure an IPv6-related address:

```
ServiceRouter(config)# ipv6 default-gateway fec0: :100/64
```

When configuring a static IPv6 prefix route, specify the host ipv6 address and prefix. <*next-hop*> is the IPv6 address of the next-hop to reach the destination prefix. The following example shows how to configure a static IPv6 prefix route:

```
ServiceRouter(config)# ipv6 route <ipv6addr/prefix> <next-hop>
```

Related Commands

Command	Description
clear ipv6	Clears IPv6 ACL counters.
show ipv6	Displays the IPv6 information.
traceroute6	Traces the route to a remote IPv6-enabled host.

kernel

To configure the kernel, use the **kernel** command in global configuration mode. To disable the kernel configuration, use the **no** form of this command.

kernel {kdb | optimization network}

no kernel {kdb | optimization network}

Syntax Description

kdb	Specifies the kernel debugger (kdb).
optimization	Enables kernel performance optimization.
network	Optimizes network performance.

Defaults

Kdb is disabled by default.

Command Modes

Global configuration (config) mode.

Usage Guidelines

Once enabled, KDB is automatically activated when kernel problems occur. Once activated, all normal functioning of the VDS-OS 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.

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** command in global configuration mode. 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 (config) mode.

Usage Guidelines

You should enable carrier detection if you connect the SE, SR, or VOSM 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 setting.

Examples

The following example shows how to specify terminal line settings:

```
ServiceEngine(config)# line console carrier-detect
```

lls

To view a long list of directory names, use the **lls** user command in user EXEC configuration mode.

lls [*directory*]

Syntax Description

directory	(Optional) Name of the directory for which you want a long list of files.

Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command provides detailed information about files and subdirectories stored in the present working directory (including size, date, time of creation, system file system (sysfs) name, and long name of the file). This information can also be viewed with the **dir** command.

Examples

The following example shows how to view a long list of directory names:

```
ServiceEngine# lls
      size          time of last change            name
-------------- ------------------------          -----------
          4096 Mon Jan 10 14:02:26 2005 <DIR>    WebsenseEnterprise
          4096 Mon Jan 10 14:02:26 2005 <DIR>    Websense_config_backup
         10203 Mon Feb 28 04:24:53 2005           WsInstallLog
          4096 Wed Feb 9 00:59:48 2005 <DIR>    core_dir
          4096 Mon Jan 10 13:49:27 2005 <DIR>    crash
           382 Tue Mar 1 03:32:13 2005           crka.log
          1604 Tue Feb 22 03:55:04 2005           dbupgrade.log
          4096 Mon Jan 10 14:02:31 2005 <DIR>    downgrade
          4096 Mon Feb 28 04:17:32 2005 <DIR>    errorlog
         53248 Tue Mar 1 03:01:53 2005 <DIR>    logs
         16384 Mon Jan 10 13:49:26 2005 <DIR>    lost+found
           438 Tue Jan 11 05:37:57 2005           new_file.xml
          8192 Tue Mar 1 00:00:00 2005 <DIR>    preload_dir
          4096 Tue Mar 1 03:26:00 2005 <DIR>    sa
         40960 Tue Mar 1 03:32:15 2005 <DIR>    service_logs
          4096 Tue Feb 22 03:51:25 2005 <DIR>    smartfilter
        384802 Mon Feb 28 03:46:00 2005           syslog.txt
         16296 Mon Feb 21 04:42:12 2005           test
          4096 Mon Jan 10 14:02:24 2005 <DIR>    var
```

Related Commands

Command	Description
dir	Displays a detailed list of files contained within the working directory, including names, sizes, and time created.
ls	Lists the files or subdirectory names within a directory.

logging

To configure system logging, use the **logging** command in global configuration mode. To disable logging functions, use the **no** form of this command.

logging {**console** {**enable** | **priority** *loglevel*} | **disk** {**enable** | **filename** *filename* | **priority** *loglevel* | **recycle** *size*} | **facility** *facility* | **host** {*hostname* | *ip_address*} [**port** *port_num* | **priority** *loglevel* | **rate-limit** *message_rate*]}

no logging {**console** {**enable** | **priority** *loglevel*} | **disk** {**enable** | **filename** *filename* | **priority** *loglevel* | **recycle** *size*} | **facility** *facility* | **host** {*hostname* | *ip_address*} [**port** *port_num* | **priority** *loglevel* | **rate-limit** *message_rate*]}

Syntax Description

console	Sets system logging to a console.
enable	Enables system logging to a console.
priority	Sets which priority level messages to send to a syslog file.
loglevel	
alert	Immediate action needed. Priority 1.
critical	Immediate action needed. Priority 2.
debug	Debugging messages. Priority 7.
emergency	System is unusable. Priority 0.
error	Error conditions. Priority 3.
information	Informational messages. Priority 6.
notice	Normal but significant conditions. Priority 5.
warning	Warning conditions. Priority 4.
disk	Sets system logging to a disk file.
enable	Enables system logging to a disk file.
filename	Sets the name of the syslog file.
filename	Specifies the name of the syslog file.
recycle	Overwrites the *syslog.txt* when it surpasses the recycle size.
size	Size of the syslog file in bytes (100000000 to 500000000).
facility	Sets the facility parameter for syslog messages.
facility	
auth	Authorization system.
daemon	System daemons.
kernel	Kernel.
local0	Local use.
local1	Local use.
local2	Local use.
local3	Local use.
local4	Local use.
local5	Local use.
local6	Local use.

local7	Local use.
mail	Mail system.
news	USENET news.
syslog	Syslog itself.
user	User process.
uucp	UUCP system.
host	Sets the system logging to a remote host.
hostname	Hostname of the remote syslog host. Specifies up to four remote syslog hosts. **Note** To specify more than one syslog host, use multiple command lines; specify one host per command.
ip_address	IP address of the remote syslog host. Specifies up to four remote syslog hosts. **Note** To specify more than one syslog host, use multiple command lines; specify one host per command.
port	(Optional) Specifies the port to be used when logging to a host.
port_num	Port to be used when logging to a host. The default port is 514.
priority	(Optional) Sets the priority level for messages when logging messages to a host. The default priority is warning.
loglevel	
alert	Immediate action needed. Priority 1.
critical	Immediate action needed. Priority 2.
debug	Debugging messages. Priority 7.
emergency	System is unusable. Priority 0.
error	Error conditions. Priority 3.
information	Informational messages. Priority 6.
notice	Normal but significant conditions. Priority 5.
warning	Warning conditions. Priority 4.
rate-limit	(Optional) Sets the rate limit (in messages per second) for sending messages to a host.
message_rate	Rate limit (in messages per second) for sending messages to the host. (0 to 10000). Setting the rate limit to 0 disables rate limiting.

Defaults

Logging: on

Priority of message for console: warning

Priority of message for log file: debug

Priority of message for a host: warning

Log file: /local1/syslog.txt

Log file recycle size: 10,000,000

Command Modes

Global configuration (config) mode.

Usage Guidelines

Use the **logging** command to set specific parameters of the system log file. System logging is always enabled internally on the SE. The system log file is located on the system file system (sysfs) partition as /local1/syslog.txt. This file contains the output from many of the VDS-OS components running on the SE, such as authentication entries, privilege levels, administrative details, and diagnostic output during the boot process.

To view information about events that have occurred in all devices in your VDS-OS network, you can use the system message log feature. When a problem occurs in the VDS-OS network, use the system message logs to diagnose and correct such problems.

The syslog.txt file on the VOSM contains information about events that have occurred on the VOSM and not on the registered nodes. The messages written to the syslog.txt file depend on specific parameters of the system log file that you have set using the **logging** global configuration command. For example, a critical error message logged on a registered node does not appear in the syslog.txt file on the VOSM because the problem never occurred on the VOSM but occurred only on the registered node. However, such an error message is displayed in the syslog.txt file on the registered node.

A disk failure syslog message is generated every time that a failed sector is accessed. Support for filtering multiple syslog messages for a single failed sector on an Integrated Drive Electronics (IDE) disk was added. Support for filtering multiple syslog messages for a single failed section for Small Computer Systems Interface (SCSI) disks and Serial Advanced Technology Attachment (SATA) disks exists.

To configure the SE to send varying levels of event messages to an external syslog host, use the **logging host** command. Logging can be configured to send various levels of messages to the console using the **logging console priority** command.

The **no logging disk recycle size** command sets the file size to the default value. Whenever the current log file size surpasses the recycle size, the log file is rotated. The log file cycles through at most five rotations, and they are saved as [*log file name*]. [*1-5*] under the same directory as the original log. The rotated log file is the one configured using the **logging disk filename** command.

Configuring System Logging to Remote Syslog Hosts

Users can log to only a single remote syslog host Use one of the following two commands to configure a single remote syslog host for an SE:

```
ServiceEngine(config)# logging host hostname
ServiceEngine(config)# logging priority priority
```

You can configure an SE to send varying levels of messages to up to four remote syslog hosts. To accommodate this, **logging host priority** *priority* global configuration command (shown above) is deprecated, and the **logging host hostname** global configuration command is extended as follows:

```
ServiceEngine(config)# [no] logging host hostname [priority priority-code | port port |
rate-limit limit]
```

where the following is true:

- *hostname* is the hostname or IP address of the remote syslog host. Specify up to four remote syslog hosts. To specify more than one syslog host, use multiple command lines; specify one host per command.
- *priority-code* is the severity level of the message that should be sent to the specified remote syslog host. The default priority code is *warning* (level 4). Each syslog host can receive a different level of event messages.

Note You can achieve syslog host redundancy by configuring multiple syslog hosts on the SE and assigning the same priority code to each configured syslog host (for example, assigning a priority code of *critical* level 2 to syslog host 1, syslog host 2, and syslog host 3).

- *port* is the destination port of the remote syslog host to which the SE is to send the messages. The default port is port 514.
- *rate-limit* specifies the number of messages that are allowed to be sent to the remote syslog host per second. To limit bandwidth and other resource consumption, messages to the remote syslog host can be rate limited. If this limit is exceeded, messages to the specified remote syslog host are dropped. There is no default rate limit, and by default all syslog messages are sent to all the configured syslog hosts. If the rate limit is exceeded, a message of the day (MOTD) is printed for any CLI EXEC shell login.

Mapping syslog Priority Levels to RealProxy Error Codes

The RealProxy system generates error messages and writes them to the RealProxy log file. These error messages are captured by the caching application and passed to the system log file. A one-to-one mapping exists between the RealProxy error codes and the syslog priority levels.

Examples

The following example shows that the SE is configured to send messages that have a priority code of "error" (level 3) to the console:

```
ServiceEngine(config)# logging console priority warnings
```

The following example shows that the SE is configured to disable sending of messages that have a priority code of "error" (level 3) to the console:

```
ServiceEngine(config)# no logging console warnings
```

The following example shows that the SE is configured to send messages that have a priority code of "error" (level 3) to the remote syslog host that has an IP address of 172.31.2.160:

```
ServiceEngine(config)#  logging host 172.31.2.160 priority error
```

Related Commands

Command	Description
clear logging	Removes all current entries from the syslog.txt file, but does not make an archive of the file.
debug	Monitors and records caching application functions.
show logging	Displays the system message log confirmation.

ls

To view a list of files or subdirectory names within a directory, use the **ls** command in EXEC configuration mode.

ls [*directory*]

Syntax Description

directory	(Optional) Name of the directory for which you want a list of files.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

To list the filenames and subdirectories within a particular directory, use the **ls** *directory* command; to list the filenames and subdirectories of the current working directory, use the **ls** command. To view the present working directory, use the **pwd** command.

Examples

The following example shows how to display a list of files within the current working directory:

```
ServiceEngine# ls
/local1
```

The following example shows how to display a list of files within the /local1 directory:

```
ServiceEngine# ls /local1
core_dir
crash
errorlog
logs
lost+found
service_logs
smartfilter
syslog.txt
```

Related Commands

Command	Description
dir	Displays a detailed list of files contained within the working directory, including names, sizes, and time created.
lls	Provides detailed information about files and subdirectories stored in the present working directory, including size, date, time of creation, system file system (sysfs) name, and long name of the file.
pwd	Displays the present working directory of the SE.

mkdir

To create a directory, use the **mkdir** command in EXEC configuration mode.

mkdir *directory*

Syntax Description

directory	Name of the directory to create.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use this command to create a new directory or subdirectory in the SE file system.

Examples

The following example shows how to create a new directory under local1:

```
ServiceEngine# mkdir /local1/mydir
```

Related Commands

Command	Description
dir	Displays a detailed list of files contained within the working directory, including names, sizes, and time created.
lls	Provides detailed information about files and subdirectories stored in the present working directory, including size, date, time of creation, system file system (sysfs) name, and long name of the file.
ls	Lists the files or subdirectory names within a directory.
pwd	Displays the present working directory of the SE.
rmdir	Removes a directory from the SE file system.

mkfile

To create a new file, use the **mkfile** command in EXEC configuration mode.

mkfile *filename*

Syntax Description

filename	Name of the file that you want to create.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use this command to create a new file in any directory of the SE.

Examples

The following example shows how to create a new file:

```
ServiceEngine# mkfile traceinfo
```

Related Commands

Command	Description
lls	Provides detailed information about files and subdirectories stored in the present working directory, including size, date, time of creation, system file system (sysfs) name, and long name of the file.
ls	Lists the files or subdirectory names within a directory.
mkdir	Creates a new directory or subdirectory in the SE file system.

model

To change the CDE250 platform model number after a remanufacturing or rescue process, use the **model** command in EXEC configuration mode.

model {**cde250-2S10** | **cde250-2S6** | **cde250-2S8** | **cde250-2S9**}

Syntax Description

cde250-2S10	Configures this platform as CDE250-2S10.
cde250-2S6	Configures this platform as CDE250-2S6.
cde250-2S8	Configures this platform as CDE250-2S8.
cde250-2S9	Configures this platform as CDE250-2S9.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use the **model** command to change the CDE250 model type. Table 2-8 shows the internal and external drives for the CDE250 models.

Table 2-8 CDE250 Model Drives

CDE250 Variation	Internal Drives	External Drives
2S6	Intel 100GB LV SSD	Intel 300GB PVR SSD x 24
2S8	Intel 100GB LV SSD	Intel 300GB PVR SSD x 24
2S9	Intel 100GB LV SSD	Intel 300GB PVR SSD x 12
2S10	Intel 100GB LV SSD	Intel 300GB PVR SSD x 24

Examples

The following example shows how to change the CDE250 to model 2S9:

```
ServiceEngine# model CDE250-2S6

This platform is already a CDE250-2S6.

ServiceEngine#
```

mount-option

To configure the mount option profile for remote storage, use the **mount-option** command in global configuration mode. To delete the configuration, use the **no** form of this command.

mount-option config-url *url* [**username** *username* **password** *password*]

no mount-option config-url *url* [**username** *username* **password** *password*]

Syntax Description

config-url	Specifies the URL for the mount option configuration file.
url	URL format [ftp|http]://domain/path/config.xml.
username	Configures the username to access the configuration file.
username	Username.
password	Configures the password to access the configuration file.
password	Password.

Command Default

None

Command Modes

Global configuration (config) mode.

Examples

The following example shows how configure the mount option:

```
ServiceEngine(config)# mount-option config-url ftp://domain/path/config.xml
```

Related Commands

Command	Description
show mount-option	Displays the mount options.

mpstat

To display processor-related statistics, use the **mpstat** command in EXEC configuration mode.

mpstat *line*

Syntax Description

line	mpstat options, -h to get help.

Command Default

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to display the mpstat list of options:

```
ServiceEngine# mpstat -h
Linux 2.6.32.52-cds-64 (W14-UCS220-3)   10/17/12        _x86_64_        (8 CPU)

01:50:50     CPU    %usr   %nice    %sys %iowait    %irq   %soft  %steal  %guest   %idle
01:50:50     all    0.01    0.11    0.12    0.02    0.00    0.00    0.00    0.00   99.74

ServiceEngine#
```

netmon

To display the transmit and receive activity on an interface, use the **netmon** command in EXEC configuration mode.

netmon *line*

Syntax Description

line	netmon options, -h to get help.

Command Default

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The netmon utility displays the transmit and receive activity on each interface in megabits per second (Mbps), bytes per second (Bps), and packets per second (pps).

Examples

The following example shows how to display the netmon list of options:

```
ServiceEngine# netmon -h
Usage: netmon [<loop-time-in-seconds>] [<iterations>]
       (runs forever if iterations not specified)
```

Related Commands

Command	Description
gulp	Captures lossless gigabit packets and writes them to disk.
netstatr	Displays the rate of change of netstat statistics.
ss	Dumps socket statistics.
tcpmon	Searches all TCP connections.

netstatr

To display the rate of change of netstat statistics, use the **netstatr** command in EXEC configuration mode.

netstatr *line*

Syntax Description

line	netmon options, -h to get help.

Command Default

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **netstatr** utility displays the rate of change, per second, of netstat statistics for a given period of time. The average rate per second is displayed, regardless of the sample period. To view the list of options, enter **netstatr -h**.

Examples

The following example shows how to display the netstart list of options:

```
ServiceEngine# netstatr -h
Usage: netstatr [-v] [<loop-time-in-seconds>] [<iterations>]
       -v verbose mode
       (default is 3 sec loop time, run forever)
```

Related Commands

Command	Description
gulp	Captures lossless gigabit packets and writes them to disk.
netmon	Displays the transmit and receive activity on an interface.
ss	Dumps socket statistics.
tcpmon	Searches all TCP connections.

no (global configuration)

To undo a command in global configuration mode or set its defaults, use the **no** form of a command in global configuration mode.

no *command*

Note The commands you can use with a VDS-OS device (including the **no** form of each command) vary based on whether the device is configured as a VOSM, SE, or SR. See Table 2-1 to identify the commands available for a specific device.

Syntax Description

command	Specifies the command type; see the Usage Guidelines section for valid values.

Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

Valid values for *command* are as follows:

access-lists	Configures access control list entries.
alarm	Configures the alarms
asset	Configures the asset tag name string.
banner	Defines a login banner.
cache	Configures cache.
cdn-select	Configures CDN select.
clock	Configures the time-of-day clock.
cms	Configures the Centralized Management System (CMS).
content-origin	Configures content origin.
device	Configures the device mode.
disk	Configures disk-related settings.
exec-timeout	Configures the EXEC timeout.
expert-mode	Configures debugshell.
external-ip	Configures up to eight external Network Address Translation (NAT) IP addresses.
ftp	Configures File Transfer Protocol (FTP) caching-related parameters.
hostname	Configures the system's network name.
http	Configures HTTP-related parameters.
interface	Configures a Gigabit Ethernet interface.

ip	Configures IP parameters.
ipv6	Configures IPv6.
kernel	Enables access to the kernel debugger.
ldap	Configures Lightweight Directory Access Protocol (LDAP) parameters.
line	Specifies terminal line settings.
logging	Configures the syslog.
mount-option	Configures the mount option profile.
ntp	Configures the Network Time Protocol (NTP).
port-channel	Configures port channel global options.
primary-interface	Configures a primary interface.
radius-server	Configures RADIUS server authentication.
service-router	Configures Service Router-related parameters.
snmp-server	Configures the Simple Network Management Protocol (SNMP) server.
ssh-key-generate	Generates the Secure Shell (SSH) host key.
sshd	Configures the SSH service.
streaming-interface	Configures the streaming interface.
tacacs	Configures Tacacs+ authentication.
tcp	Configures global TCP parameters.
telnet	Configures Telnet services.
transaction-logs	Configures the transaction logging.
url-signature	Configures an encryption key to use when signing a URL.
username	Establishes username authentication.
VOSM	Configures the VOSM settings.
web-engine	Configures the Web Engine parameters.

Use the **no** command to disable functions or negate a command. If you need to negate a specific command, such as the default gateway IP address, you must include the specific string in your command, such as **no ip default-gateway** *ip-address*.

no (interface configuration)

To negate an interface configuration mode, use the **no** command in interface configuration mode.

no {**autosense** | **bandwidth** {**10-10** | **100-100** | **1000-1000** | **10000-10000**} | **description** | **full-duplex** | **half-duplex** | **ip** {**access-group** {*num* {**in** | **out**} | **name** {**in** | **out**} | **address** *ip-addr*} | **ipv6** {**access-group** {*num* {**in** | **out**} | **name** {**in** | **out**} | **address** *ip-addr*} | **lacp** | **mtu** | **shutdown** | **standby** *group-num* [**priority** *interface*]}

Syntax Description

autosense	Negates an autosense interface.
bandwidth	Negates a bandwidth interface.
10-10	Specifies 10 Mb per second bandwidth.
100-100	Specifies 100 Mb per second bandwidth.
1000-1000	Specifies 1000 Mb per second bandwidth. **Note** Not available on all ports.
10000-10000	Specifies 10000 Mb per second bandwidth. **Note** Not available on all ports.
description	Negates a description-specific interface.
full-duplex	Negates a full-duplex interface.
half-duplex	Negates a half-duplex interface.
ip	Negates Internet Protocol configuration commands.
access-group	Specifies access control for packets.
num	IP access list number (standard or extended).
in	Inbound packets.
out	Outbound packets.
name	Access list name.
address	Sets the IP address of the interface.
ip-addr	Interface IP address.
netmask	Interface netmask.
range	Sets the IP address range.
low-num	IP address low range of the interface.
high-num	IP address high range of the interface.
ipv6	Negates the interface IPv6 configuration commands.
lacp	Negates the Link Aggregation Control Protocol.
mtu	Sets the interface Maximum Transmission Unit.
size	Maximum transmission unit (MTU) size in bytes.
shutdown	Shuts down the specific portchannel interface.
standby	Negates the standby interface configuration commands.
group-num	Specifies the standby group number.
priority	Sets the priority of the interface for the standby group.
interface	Interface priority.

Defaults **Priority**: 100.

Command Modes Interface configuration (config-if) mode.

Related Commands

Command	Description
interface	Configures a Gigabit Ethernet or port channel interface.
show interface	Displays the hardware interface information.
show running-config	Displays the current running configuration information on the terminal.
show startup-config	Displays the startup configuration.

ntp

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

ntp server {*ip_address* | *hostname*} [*ip_addresses* | *hostnames*]

no ntp server {*ip_address* | *hostname*} [*ip_addresses* | *hostnames*]

Syntax Description

server	Sets the NTP server IP address.
ip_address	NTP server IP address.
hostname	NTP server hostname.
ip_addresses	(Optional) IP address of the time server providing the clock synchronization (maximum of four).
hostnames	(Optional) Hostname of the time server providing the clock synchronization (maximum of four).

Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

Use this command to synchronize the SE, SR or VOSM clock with the specified NTP server. The **ntp server** command enables NTP servers for timekeeping purposes and is the only way to synchronize the system clock with a time server.

When you synchronize the VOSM clock with an NTP server, there is a possibility of all devices registered with the VOSM being shown as offline and then reverted to online status. This situation can occur when synchronization with the NTP server sets the VOSM clock forward in time by an interval greater than at least two polling intervals or when the software clock on the VOSM is changed by a similar value using the **clock** command in EXEC configuration mode. The VOSM determines the status of devices in the VDS-OS network depending on when it was last contacted by the devices for a getUpdate request. If you set the VOSM clock ahead in time, you have added that amount of time to the period since the VOSM received the last getUpdate request. However, it is only a transient effect. Once the devices contact the VOSM for their next getUpdate request after the clock setting change, the VOSM GUI reports the status of all devices correctly.

Examples

The following example shows how to configure the IP address of the time server providing the clock synchronization:

```
ServiceEngine(config)# ntp server 172.16.22.44
```

The following example shows how to reset the time server providing the clock synchronization:

```
ServiceEngine(config)# no ntp server 172.16.22.44
```

Related Commands

Command	Description
clock	Sets or clears clock functions or updates the calendar.
show clock	Displays the system clock.
show ntp	Displays the Network Time Protocol parameters.

ntpdate

To set the software clock (time and date) using a Network Time Protocol (NTP) server, use the **ntpdate** command in EXEC configuration mode.

ntpdate {*hostname* | *ip_address*}

Syntax Description

hostname	NTP hostname.
ip_address	NTP server IP address.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use NTP to find the current time of day and set the SE current time to match. The **ntpdate** command synchronizes the software clock with the hardware clock.

Examples

The following example shows how to set the software clock of the SE using an NTP server:

```
ServiceEngine# ntpdate 10.11.23.40
```

Related Commands

Command	Description
clock set	Sets the time and date.
show clock	Displays the system clock.

ping

To send echo packets for diagnosing basic network connectivity on networks, use the **ping** command in EXEC configuration mode.

ping {*hostname* | *ip_address*}

Syntax Description

hostname	Hostname of system to ping.
ip_address	IP address of system to ping.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

To use this command with the *hostname* argument, be sure that Domain Name System (DNS) functionality is configured on your SE. To force the timeout of a nonresponsive host or to eliminate a loop cycle, press **Ctrl-C**.

Following are sample results of the **ping** command:

- Normal response—The normal response occurs in 1 to 10 seconds, depending on network traffic.
- Destination does not respond—If the host does not respond, a `no answer from host` message appears in 10 seconds.
- Destination unreachable—The gateway for this destination indicates that the destination is unreachable.
- Network or host unreachable—The SE found no corresponding entry in the route table.

Examples

The following example shows how to test the basic network connectivity with a host:

```
ServiceEngine# ping 172.19.131.189
PING 172.19.131.189 (172.19.131.189) from 10.1.1.21 : 56(84) bytes of
data.
64 bytes from 172.19.131.189: icmp_seq=0 ttl=249 time=613 usec
64 bytes from 172.19.131.189: icmp_seq=1 ttl=249 time=485 usec
64 bytes from 172.19.131.189: icmp_seq=2 ttl=249 time=494 usec
64 bytes from 172.19.131.189: icmp_seq=3 ttl=249 time=510 usec
64 bytes from 172.19.131.189: icmp_seq=4 ttl=249 time=493 usec

--- 172.19.131.189 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.485/0.519/0.613/0.047 ms
ServiceEngine#
```

ping6

To ping the IPv6 address, use the **ping6** command in EXEC configuration mode.

ping6 *line ip_address*

Syntax Description

line	Destination Host or IP Address.
ip_address	IP address of system to ping.

Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to ping the IPv6 address:

```
ServiceEngine# ping6 fec0: :100/64
```

Related Commands

Command	Description
ping	Sends echo packets for diagnosing basic network connectivity on networks.

port-channel

To configure the port channel load balancing, use the **port-channel** command in global configuration mode. To disable load balancing, use the **no** form of this command.

port-channel load-balance {**dst-ip** | **dst-mac** | **dst-mixed-ip-port** | **dst-port** | **round-robin** | **src-dst-mac** | **src-dst-mixed-ip-port** | **src-dst-port** | **src-ip** | **src-mixed-ip-port** | **src-port**}

no port-channel load-balance

Syntax Description

load-balance	Configures the load balancing method.
dst-ip	Specifies the load balancing method using destination IP addresses.
dst-mac	Specifies the load balancing method using destination Media Access Control (MAC) addresses.
dst-mixed-ip-port	Specifies the destination IP Addr and Layer 4 port.
dst-port	Specifies the load balancing method using destination Layer 4 port.
round-robin	Specifies the load balancing method using round-robin sequential, cyclical resource allocation (each interface in the channel group).
src-dst-mac	Specifies the load balancing method using source and destination MAC address.
src-dst-mixed-ip-port	Specifies the source and destination IP Addr and Layer 4 port.
src-dst-port	Specifies the load balancing method using source and destination port.
src-ip	Specifies the load balancingmethod using the source IP address.
src-mixed-ip-port	Specifies the source and destination IP Addr and Layer 4 port.
src-port	Specifies the load balancing method using source Layer 4 port.

Defaults

Round-robin is the default load balancing method.

Command Modes

Global configuration (config) mode.

Usage Guidelines

The **port-channel load-balance** command configures one of three load balancing algorithms and provides flexibility in choosing interfaces when an Ethernet frame is sent. The **round-robin** keyword allows evenly balanced usage of identical network interfaces in a channel group. Because this command takes effect globally, if two channel groups are configured, they must use the same load balancing.

The other balancing options give you the flexibility to choose specific interfaces (by IP address, MAC address, port) when sending an Ethernet frame. The source and destination options, while calculating the outgoing interface, take into account both the source and destination (MAC address or port).

Because the VDS-OS software normally starts IP packets or Ethernet frames, it does not support hashing based on the source IP address and source MAC address. The **round-robin** keyword is the default load balancing algorithm to evenly distribute traffic among several identical network interfaces.

To remove a port channel, use the **no port-channel interface PortChannel** command.

Note Ingress traffic from Network-Attached Storage (NAS) mounts is not distributed evenly over port channels. Separate interfaces can be used for NAS outside of the port-channel configuration to achieve better load balancing. Ingress traffic to the VDS-OS is determined by the switch, this applies to all application traffic over port channels.

For load balancing, the round robin method alone is not supported with LACP.

Examples

The following example shows how to configure the round-robin load balancing method on an SE:

```
ServiceEngine(config)# port-channel load-balance round-robin
```

Related Commands

Command	Description
interface	Configures a Gigabit Ethernet or port-channel interface

primary-interface

To configure the primary interface for the VDS-OS network, use the **primary-interface** command in global configuration mode. Use the **no** form of the command to remove the configured primary interface.

primary-interface {**GigabitEthernet** *1-2/port* | **PortChannel** *1-2* | **Standby** *group_num*}

no primary-interface {**GigabitEthernet** *1-2/port* | **PortChannel** *1-2* | **Standby** *group_num*}

Syntax Description

GigabitEthernet	Selects a Gigabit Ethernet interface as the VDS-OS network primary interface.
1-2/	Gigabit Ethernet slot numbers 1 or 2.
port	Port number of the Gigabit Ethernet interface.
PortChannel	Selects a port channel interface as the VDS-OS network primary interface.
1-2	Port channel number 1 or 2.
Standby	Selects a standby group as the VDS-OS network primary interface.
group_num	Standby group number.

Defaults

The default primary interface is the first operational interface on which a link beat is detected. Interfaces with lower-number IDs are polled first (for example, GigabitEthernet 0/0 is checked before 1/0). Primary interface configuration is required for the proper functioning of the Centralized Management System (CMS). After devices are registered to the VOSM, the VOSM uses the configured primary interface to communicated with the registered devices.

You cannot enable the VDS-OS network without specifying the primary interface. Also, you must have chosen the primary interface before you enable the CMS. The primary interface can be changed without disabling the VDS-OS network. The primary interface specifies the default route for an interface. To change the primary interface, choose a different interface as the primary interface.

Note Whenever the IP address of the primary interface is changed, the Domain Name System (DNS) server must be restarted.

You can select a standby interface as the primary interface (you can enter the **primary-interface Standby** *group_num* command) to specify a standby group as the primary interface on an SE.

Command Modes

Global configuration (config) mode.

Usage Guidelines

The **primary-interface** command in global configuration mode allows the administrator to specify the primary interface for the VDS-OS network.

The primary interface can be changed without disabling the VDS-OS network. To change the primary interface, re-enter the command string and specify a different interface.

Note If you use the **restore factory-default preserve basic-config** command, the configuration for the primary interface is not preserved. On a device in a VDS-OS network, if you want to re-enable the VDS-OS network after using the **restore factory-default preserve basic-config** command**,** make sure to reconfigure the primary interface after the factory defaults are restored.

Examples

The following example shows how to specify the Gigabit Ethernet slot 1 port 0 as the primary interface on an SE:

```
ServiceEngine(config)# primary-interface GigabitEthernet 1/0
```

The following example shows how to specify the Gigabit Ethernet slot 2 port 0 as the primary interface on an SE:

```
ServiceEngine(config)# primary-interface GigabitEthernet 2/0
```

pwd

To view the present working directory, use the **pwd** command in EXEC configuration mode.

pwd

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use this command to display the present working directory of the SE.

Examples

The following example shows how to view the present working directory:

```
ServiceEngine# pwd
/local1
```

Related Commands

Command	Description
cd	Changes from one directory to another directory.
dir	Displays a detailed list of files contained within the working directory, including names, sizes, and time created.
lls	Provides detailed information about files and subdirectories stored in the present working directory, including size, date, time of creation, system file system (sysfs) name, and long name of the file.
ls	Lists the files or subdirectory names within a directory.

radius-server

To configure RADIUS authentication parameters, use the r**adius-server** command in global configuration mode. To disable RADIUS authentication parameters, use the **no** form of this command.

radius-server {**enable | host** {*hostname* | *host_ipaddr*} [**auth-port** *port*] | **key** *keyword* | **redirect** {**enable | message** *reply* **location** *url*} | **retransmit** *retries* | **timeout** *seconds*}

no radius-server {**enable | host** {*hostname* | *host_ipaddr*} | **key** | **redirect** {**enable | message** *reply* **location** *url*} | **retransmit | timeout**}

Syntax Description

enable	Enables HTTP RADIUS authentication.
host	Specifies a RADIUS server.
hostname	Hostname of the RADIUS server.
host_ipaddr	IP address of the RADIUS server.
auth-port	(Optional) Sets the UDP port for the RADIUS Authentication Server.
port	UDP port number (from 1 to 65535). The default is 1645.
key	Specifies the encryption key shared with the RADIUS server.
keyword	Text of the shared key (maximum of 15 characters).
redirect	Redirects the response if an authentication request fails.
enable	Enables the redirect feature.
message	Replies with an authentication failure message.
reply	Reply message text string (maximum of 24 characters).
location	Sets the HTML page location, for example, http://www.cisco.com.
url	URL destination of authentication failure instructions.
retransmit	Specifies the number of transmission attempts to an active server.
retries	Number of transmission attempts for a transaction (from 1 to 3).
timeout	Time to wait for a RADIUS server to reply.
seconds	Wait time in seconds (from 1 to 20).

Defaults

auth-port *port*: UDP port 1645

retransmit *retries*: 2

timeout *seconds*: 5

Command Modes

Global configuration (config) mode.

Usage Guidelines

RADIUS is a client/server authentication and authorization access protocol used by a VDS-OS network device to authenticate users attempting to connect to a network device. The VDS-OS network device functions as a client, passing user information to one or more RADIUS servers. The VDS-OS network

device permits or denies network access to a user based on the response that it receives from one or more RADIUS servers. RADIUS uses the User Datagram Protocol (UDP) for transport between the RADIUS client and server.

You can configure a RADIUS key on the client and server. If you configure a key on the client, it must be the same as the one configured on the RADIUS servers. The RADIUS clients and servers use the key to encrypt all RADIUS packets sent. If you do not configure a RADIUS key, packets are not encrypted. The key itself is never sent over the network.

Note For more information about how the RADIUS protocol operates, see RFC 2138, *Remote Authentication Dial In User Service (RADIUS)*.

RADIUS authentication usually occurs in these instances:

- Administrative login authentication—When an administrator first logs in to the SE to configure the SE for monitoring, configuration, or troubleshooting purposes. For more information, see the "Enabling and Disabling Administrative Login Authentication Through RADIUS" section on page 2-169.
- HTTP request authentication—When an end user sends a service request that requires privileged access to content that is served by the SE. For more information, see the "Configuring RADIUS Authentication of HTTP Requests" section on page 2-170.

RADIUS authentication is disabled by default. You can enable RADIUS authentication and other authentication methods at the same time. You can also specify which method to use first.

To configure RADIUS parameters, use the **radius-server** command in global configuration mode. To disable RADIUS authentication parameters, use the **no** form of this command.

The **redirect** keyword of the **radius-server** command redirects an authentication response to a different Authentication Server if an authentication request using the RADIUS server fails.

Note The following **rule** command is relevant to RADIUS authentication only if the **redirect** keyword has been configured.

To exclude domains from RADIUS authentication, use the **rule no-auth domain** command. RADIUS authentication takes place only if the site requested does not match the specified pattern.

Enabling and Disabling Administrative Login Authentication Through RADIUS

When configuring an SE to use RADIUS to authenticate and authorize administrative login requests, follow these guidelines:

- By default, RADIUS authentication and authorization is disabled on an SE.
- Before enabling RADIUS authentication on the SE, you must specify at least one RADIUS server for the SE to use.
- You can enable RADIUS authentication and other authentication methods at the same time. You can specify which method to use first using the **primary** keyword. When local authentication is disabled, if you disable all other authentication methods, local authentication is re-enabled automatically.
- You can use the VOSM GUI or the CLI to enable RADIUS authentication on an SE.

Tip From the VOSM GUI, choose **Devices > General Settings > Authentication**. Use the displayed Authentication Configuration window.

To use the SE CLI to enable RADIUS authentication on an SE, enable RADIUS authentication for normal login mode by entering the **authentication login radius** command in global configuration mode as follows:

```
ServiceEngine(config)# authentication login radius enable [primary] [secondary]
```

Use the **authentication configuration radius** command in global configuration mode to enable RADIUS authorization as follows:

```
ServiceEngine(config)# authentication configuration radius enable [primary] [secondary]
```

Note To disable RADIUS authentication and authorization on an SE, use the **no radius-server enable** command.

Configuring RADIUS Authentication of HTTP Requests

To configure RADIUS authentication for HTTP requests on an SE, configure the RADIUS server settings on the SE and enable RADIUS authentication for HTTP requests on the SE using the **radius-server** command in global configuration mode.

Examples

The following example shows how to enable the RADIUS client, specify a RADIUS server, specify the RADIUS key, accept retransmit defaults, and excludes the domain name, mydomain.net, from RADIUS authentication. You can verify the configuration with the **show radius-server** and **show rule all** commands.

```
ServiceEngine(config)# radius-server enable
ServiceEngine(config)# radius-server host 172.16.90.121
ServiceEngine(config)# radius-server key myradiuskey
ServiceEngine(config)# rule action no-auth pattern-list 2
ServiceEngine(config)# rule pattern-list 2 domain mydomain.net


ServiceEngine# show radius-server
Login Authentication for Console/Telnet/Ftp/SSH Session: enabled
Configuration Authentication for Console/Telnet/Ftp/SSH Session: enabled (secondary)

Radius Configuration:
---------------------
Radius Authentication is on
Timeout = 5
Retransmit = 2
Key = ****
Radius Redirect is off
There is no URL to authentication failure instructions
Servers
-------
IP 172.16.90.121 Port = 1645

ServiceEngine# show rule all
Rules Template Configuration
----------------------------
Rule Processing Enabled
rule no-auth domain mydomain.net
```

The following example disables RADIUS authentication on the SE:

```
ServiceEngine(config)# no radius-server enable
```

The following example shows how to force the SE to try RADIUS authentication first:

```
ServiceEngine(config)# authentication login radius enable primary
```

Related Commands

Command	Description
debug authentication user	Debugs the user login against the system authentication.
rule	Sets the rules by which the SE filters HTTP, HTTPS, and Real-Time Streaming Protocol (RTSP) traffic.
show radius-server	Displays RADIUS information.

reload

To halt and perform a cold restart on the SE, use the **reload** command in EXEC configuration mode.

reload [**force**]

Syntax Description

force	(Optional) Forces a reboot without further prompting.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

To reboot the SE, use the **reload** command. If the current running configuration is different from the startup configuration and if the configuration changes are not saved to flash memory, you are prompted to save the current running configuration parameters to the startup configuration.

To save any file system contents to disk from memory before a restart, use the **cache synchronize** command.

Examples

The following example shows how to reload the SE after you have saved the configuration changes.

```
ServiceEngine# reload
System configuration has been modified. Save? [ yes ] :yes
Proceed with reload? [ confirm ] yes
Shutting down all services, will timeout in 15 minutes.
reload in progress.....
```

The following example forces a reboot on the SE:

```
ServiceEngine# reload force
```

Related Commands

Command	Description
cache synchronize	Saves any file system contents to disk from memory before a restart.
write	Saves startup configurations.
write erase	Erases the startup configuration from nonvolatile random-access memory (NVRAM).

rename

To rename a file on the SE, use the **rename** command in EXEC configuration mode.

rename *old_filename new_filename*

Syntax Description

old_filename	Original filename.
new_filename	New filename.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use this command to rename any system file system (sysfs) file without making a copy of the file.

Examples

The following example renames a file named errlog.txt as old_errlog.txt:

```
ServiceEngine# rename errlog.txt old_errlog.txt
```

Related Commands

Command	Description
cpfile	Creates a copy of a file.

restore

To restore the device to its manufactured default status, removing the user data from the disk and flash memory, use the **restore** command in EXEC configuration mode. This command erases all existing content on the device.

restore factory-default [**preserve basic-config**]

Syntax Description

factory-default	Resets the device configuration and data to their manufactured default status.
preserve	(Optional) Preserves certain configurations and data on the device.
basic-config	(Optional) Selects basic network configurations.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use this command to restore data on disk and in flash memory to the factory default, while preserving particular time stamp evaluation data. You need to enter this command from the root directory, or else the following error message is displayed:

```
ServiceEngine# restore factory-default

Need to cd to / before issuing this command

Command aborted.
SERVICEENGINE#
```

Be sure to back up the VOSM database and copy the backup file to a safe location that is separate from that of the VOSM, or change over from the primary to a standby VOSM before you use the **restore factory-default** command on your primary VOSM. The primary VOSM operation must be halted before proceeding with **backup** and **restore** commands.

Caution This command erases user-specified configuration information stored in the flash image and removes the data on the disk, the user-defined disk partitions, and the entire VOSM database. User-defined disk partitions that are removed include the sysfs and cdnfs partitions. The configuration being removed includes the starting configuration of the device.

By removing the VOSM database, all configuration records for the entire VDS-OS network are deleted. If you do not have a valid backup file or a standby VOSM, you must use the **cms deregister force** command and reregister every SE and SR after you have reconfigured the VOSM, because all previously configured data is lost.

If you used your standby VOSM to store the database while you reconfigured the primary, you can simply register the former primary as a new standby VOSM.

If you created a backup file while you configured the primary VOSM, you can copy the backup file to this newly reconfigured VOSM and use the **cms database restore** command.

Caution If you upgraded your software after you received your software recovery CD-ROM, using the CD-ROM software images may downgrade your system.

VDS-OS software consists of three basic components:

- Disk-based software
- Flash-based software
- Hardware platform cookie (stored in flash memory)

All these components must be correctly installed for VDS-OS software to work properly.

Examples

The following two examples show the results of using the **restore factory-default** and **restore factory-default preserve basic-config** commands. Because configuration parameters and data are lost, prompts are given before initiating the restore operation to ensure that you want to proceed.

Note If you use the **restore factory-default preserve basic-config** command, the configuration for the primary interface is not preserved. If you want to re-enable the VDS-OS network after using the **restore factory-default preserve basic-config** command, reconfigure the primary interface after the factory defaults have been restored.

```
VOSM# restore factory-default
This command will wipe out all of data on the disks
and wipe out VDS-OS CLI configurations you have ever made.
If the box is in evaluation period of certain product,
the evaluation process will not be affected though.

It is highly recommended that you stop all active services
before this command is run.

Are you sure you want to go ahead? [ yes/no ]

VOSM# restore factory-default preserve basic-config
This command will wipe out all of data on the disks
and all of VDS-OS CLI configurations except basic network
configurations for keeping the device online.
The to-be-preserved configurations are network interfaces,
default gateway, domain name, name server and hostname.
If the box is in evaluation period of certain product,
the evaluation process will not be affected.
It is highly recommended that you stop all active services
before this command is run.

Are you sure you want to go ahead? [ yes/no ]
```

Note You can enter basic configuration parameters (such as the IP address, hostname, and name server) at this point or later through entries in the command-line interface.

The following example shows that entering the **show disks** command after the **restore** command verifies that the **restore** command has removed data from the partitioned file systems (sysfs and cdnfs):

```
ServiceEngine# show disks

SYSFS        0.0GB        0.0%
```

```
CDNFS        0.0GB         0.0%
FREE         29.9GB       100.0%
```

Because flash memory configurations were removed after the **restore** command was used, the **show startup-config** command does not return any flash memory data. The **show running-config** command returns the default running configurations.

Related Commands

Command	Description
cms database backup	Backs up the existing management database for the VOSM.
cms database restore	Restores the database management tables using the backup local filename.
show disks	Displays the names of the disks currently attached to the SE.
show running-config	Displays the current running configuration information on the terminal.
show startup-config	Displays the startup configuration.

rmdir

To delete a directory, use the **rmdir** command in EXEC configuration mode.

rmdir *directory*

Syntax Description

directory	Name of the directory that you want to delete.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use this command to remove any directory from the SE file system. The **rmdir** command removes only empty directories.

Examples

The following example shows how to remove the oldfiles directory under /local1:

```
ServiceEngine# rmdir /local1/oldfiles
```

Related Commands

Command	Description
lls	Provides detailed information about files and subdirectories stored in the present working directory, including size, date, time of creation, system file system (sysfs) name, and long name of the file.
ls	Lists the files or subdirectory names within a directory.
mkdir	Creates a new directory or subdirectory in the SE file system.

script

To execute a script provided by Cisco or check the script for errors, use the **script** command in EXEC configuration mode.

script {**check** | **execute**} *file_name*

Syntax Description

check	Checks the validity of the script.
execute	Executes the script. The script file must be a system file system (sysfs) file in the current directory.
file_name	Name of the script file.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **script** command in EXEC configuration mode opens the script utility, which allows you to execute scripts supplied by Cisco or check errors in those scripts. The script utility can read standard terminal input from the user if the script you run requires inputs from the user.

Note The script utility is designed to run only in scripts supplied by Cisco. You cannot execute script files that lack Cisco signatures or that have been corrupted or modified.

Examples

The following example shows how to check for errors in the script file foo.script:

```
ServiceEngine# script check foo.script

 Script file foo.script is valid.
```

service

To specify the type of service, use the **service** command in EXEC configuration mode.

On the VOSM:

service csm restart

On the SE:

service {**capture-controller restart** | **csm restart** | **web-engine restart**}

On the SR:

service {**cms restart** | **service-router restart**}

Syntax Description

capture-controller	Specifies Capture Controller services.
csm	Specifies CMS services.
restart	Restarts the specified services.
service-router	Specifies Service Router services.
web-engine	Specifies Web Engine services.

Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to restart Web Engine service:

```
ServiceEngine# service web-engine restart
The service Web Engine has been restarted successfully!
ServiceEngine#
```

service-router

To configure service routing, use the **service-router** command in global configuration mode. To disable last-resort routing, use the **no** form of this command.

On the SE:

service-router {**keepalive-interval** *num* | **service-monitor** {**augmentation-alarm enable** | **license-universal enable** | **number-of-samples** {**all** *num* | **cpu** *num* | **disk** *num* | **kmemory** *num* | **memory** *num* | **nic** *num*} | **sample-period** {**all** *num* | **cpu** *num* | **disk** *num* | **kmemory** *num* | **memory** *num* | **nic** *num*} | **threshold** {**augmentation** *num* | **burstcnt** *num* | **cpu** *num* | **disk** *num* | **faildisk** *num* | **kmemory** *num* | **memory** *num* |**nic** *num*} | **transaction-log enable** | **type** {**all** | **cpu** | **disk** | **kmemory** | **memory** | **nic**}}}

no service-router {**keepalive-interval** *num* | **service-monitor** {**augmentation-alarm enable** | **license-universal enable** | **number-of-samples** {**all** *num* | **cpu** *num* | **disk** *num* | **kmemory** *num* | **memory** *num* | **nic** *num*} | **sample-period** {**all** *num* | **cpu** *num* | **disk** *num* | **kmemory** *num* | **memory** *num* | **nic** *num*} | **threshold** {**augmentation** *num* | **burstcnt** *num* | **cpu** *num* | **disk** *num* | **faildisk** *num* | **kmemory** *num* | **memory** *num* |**nic** *num*} | **transaction-log enable** | **type** {**all** | **cpu** | **disk** | **kmemory** | **memory** | **nic**}}}

On the SR:

service-router service-monitor {**augmentation-alarm enable** | **number-of-samples** {**all** *num* | **cpu** *num* | **disk** *num* | **kmemory** *num* | **memory** *num*} | **sample-period** {**all** *num* | **cpu** *num* | **disk** *num* | **kmemory** *num* | **memory** *num*} | **threshold** {**augmentation** *num* | **cpu** *num* | **disk** *num* | **faildisk** *num* | **kmemory** *num* | **memory** *num*} | **type** {**all** | **cpu** | **disk** | **kmemory** | **memory**}}

no service-router service-monitor {**augmentation-alarm enable** | **number-of-samples** {**all** *num* | **cpu** *num* | **disk** *num* | **kmemory** *num* | **memory** *num*} | **sample-period** {**all** *num* | **cpu** *num* | **disk** *num* | **kmemory** *num* | **memory** *num*} | **threshold** {**augmentation** *num* | **cpu** *num* | **disk** *num* | **faildisk** *num* | **kmemory** *num* | **memory** *num*} | **type** {**all** | **cpu** | **disk** | **kmemory** | **memory**}}

On the VOSM:

service-router {**lastresort** {**domain** *name* {**allow all** | **alternate** *name port_num*} | **error-domain** *name* **error-file** *port_num* | **translator** *ip_address port_num*} | **redirect-burst-control** {**enable** | **rate** *num*} | **service-monitor** {**augmentation-alarm enable** | **number-of-samples** {**all** *num* | **cpu** *num* | **disk** *num* | **kmemory** *num* | **memory** *num*}} | **threshold** {**augmentation** *num* | **cpu** *num* | **disk** *num* | **kmemory** *num* | **memory** *num* | **transaction-log enable**}}

no service-router {**lastresort** {**domain** *name* {**allow all** | **alternate** *name port_num*} | **error-domain** *name* **error-file** *port_num* | **translator** *ip_address port_num*} | **redirect-burst-control** {**enable** | **rate** *num*} | **ip-redirect**} | **service-monitor** {**augmentation-alarm enable** | **number-of-samples** {**all** *num* | **cpu** *num* | **disk** *num* | **kmemory** *num* | **memory** *num*}} | **threshold** {**augmentation** *num* | **cpu** *num* | **disk** *num* | **kmemory** *num* | **memory** *num* | **transaction-log enable**}}

Syntax Description

keepalive-interval	Specifies the SR keepalive interval in seconds.
keepalive_interval _num	Number of seconds. The range is from 1 to 120.
service-monitor	Configures Service Monitor related parameters.

augmentation-alarm	Alarm for checking the device level loads.
enable	Enables the augmentation alarm.
license-universal	Universal license feature to clear all alarms for Protocol Engines.
enable	Enables the universal license feature.
number-of-samples	Counts the latest sampled values to be used when calculating average.
all	Sets to all monitor types.
num	Count of latest sampled values to be used when calculating average. The range is from 1 to 120.
cpu	Enables the monitor CPU load.
disk	Sets the disk monitor type.
kmemory	Sets the monitor kernel memory type.
memory	Sets the monitor memory type.
nic	Sets the Network Interface Card monitor type.
sample-period	Configures the time interval, in seconds, between two consecutive samples.
num	Time interval between two consecutive samples, in seconds. The range is from 1 to 60.
threshold	Configures threshold values.
augmentation	Applies the Augmentation alarm threshold as a percentage of the device parameter threshold.
num	Configures the Augmentation threshold values in percentage (1 to 100).
burstcnt	Configures the Protocol Engine Burst License Control monitor type.
num	Protocol Engine Burst License Control threshold value.
faildisk	Sets the disk failure monitor type.
num	Configures the Disk Failure Count threshold percentage (1-100). The default is 75 percent.
type	Configures the type to be monitored.
enable	Enables the CDN Selector.
enable	Enables content based routing.
redundant	Specifies the number of redundant copies of the content.
num	Number of redundant copies of the content. The range is from 1 to 4.
lastresort	Configures the lastresort domain.
domain	Configures the domain.
name	Domain name.
allow	Allows the client to be routed through an alternate domain or origin service.
all	Allows all requests.
alternate	Configures an alternate domain.
name	Alternate domain name.
error-domain	Configures error domain.
name	Error domain name.
translator	Configures the external translator IP address.
ip_address	External translator IP address.

port	(Optional) Specifies the port number.
port_num	Port number (1-65535).
error-file	Configures error file name.
port_num	Error file name.
proximity-server	Configures proximity server IP address and port.
ip_address	IP address of proximity server.
redirect-burst-control	Configures the redirect burst control.
enable	Enables redirect burst control.
rate	Configures the redirect burst control rate (requests per second).
num	Redirect burst control rate. The range is from 1 to 100000.
service-monitor	Configures service monitor parameters.
number-of-samples	Counts the latest sampled values to be used when calculating average.
all	Allows all monitor types.
num	Count of latest sampled values to be used when calculating average. The range is from 1 to 120.
cpu	Sets the CPU monitor type.
disk	Sets the disk monitor type.
kmemory	Sets the monitor kernel memory.
memory	Sets the monitor memory.
faildisk	Sets the disk failure monitor type.
sample-period	Configures the time interval between two consecutive samples.
threshold	Configures threshold values.
transaction-log	Configures Transaction logging for the Service Monitor.
enable	Enables transaction logging for the Service Monitor.
type	Configures the type to be monitored.

Defaults

keepalive-interval: 2

redundant copies: 1

dns-ttl: 60

burstcnt: 1

location cache timeout: 691200 seconds (8 days)

proximity cache timeout: 1800

sample-period: 1

nic sample-period: 3

number of samples: 2

faildisk: 75 percent

augmentation-alarm: disabled

transaction-logs: disabled

port number: 80

Command Modes Global configuration (config) mode.

Usage Guidelines To configure last-resort routing, use the **service-router** command in global configuration mode, where domain is the service routing domain name, and alternate is where to route requests.

Last-resort routing is applicable when load-based routing is enabled and all SEs have exceeded their thresholds or all SEs in the domain are offline. The SR can redirect requests to a configurable alternate domain when all SEs serving a client network region are overloaded.

Note If the last-resort domain is not configured and the SE thresholds are exceeded, requests are redirected to the origin service.

Augmentation Alarms

Augmentation alarms on the Service Monitor are soft alarms that send alerts before the threshold is reached. These alarms are applicable to all devices—Service Engines, Service Routers and VOSMs. Augmentation thresholds apply to device and Protocol Engine parameters.

Note For system disks (disks that contain SYSTEM partitions), only when all system disks are bad is the disk failure augmentation and threshold alarms raised. The disk fail threshold does not apply to system disks. The threshold only applies to CDS network file system (CDNFS) disks, which is also the case for the augmentation thresholds. This is because the system disks use RAID1. There is a separate alarm for bad RAID. With the RAID system, if the critical primary disk fails, the other mirrored disk (mirroring only occurs for SYSTEM partitions) seamlessly continues operation. However, if the disk drive that is marked bad is a critical disk drive (by definition this is a disk with a SYSTEM partition), the redundancy of the system disks for this device is affected.

As the **show disk** details command output reports, if disks have both SYSTEM and CDNFS partitions, they are treated as only system disks, which means they are not included in the accounting of the CDNFS disk calculation.

Cross Domain Support

When a client requests the content from a portal and the content then makes a request to a different remote domain (or origin service), the request cannot be served unless the origin service or the remote domain has a crossdomain.xml that grants access to the original portal to continue with the streaming.

For example, a client request for abc.com/streaming.html (which has the content), makes a request for VDS-OS-origin.com/vod/sample.flv (which is a different domain), then the client must request a crossdomain.xml. The crossdomain.xml allows access to abc.com and can then stream sample.flv. If the VDS-OS-origin.com does not have crossdomain.xml, then the request is denied.

Note In the case of Flash, the request is made for crossdomain.xml. In the case of Silverlight the request is made for clientaccesspolicy.xml.

Instead of directly going to VDS-OS-origin.com, the request first comes to the Service Router. So when the request for crossdomain.xml comes to the Service Router, it is served to the client. This xml grants access to the portal for the file requested. So the client then sends the request for the file which is served.

Note For Silverlight the client access policy is requested only when web service calls are made. Depending on the client player, for both Silverlight and Flash applications, the clientaccesspolicy.xml and crossdomain.xml need to be provisioned on the origin service.

FLVPlaybackComponent does not currently crossdomain requests for video files. The crossdomain request is issued only when a query string is present. In such cases, the video gets downloaded but does not play.

The number of the HTTP Requests (normal) in Request Received (**show statistics service-router summary**) should increase.

Last-Resort Routing

Last-resort routing is not supported when dns-based-redirect is enabled.

Configuring the license-universal Command

Universal license is like a regular license but with higher BW and it applies to all PEs. When the user buys a universal license and configures this command, alarm data for all PEs is cleared. Thereafter monitoring of the PEs continues as usual for any future alarms. If universal license was already configured upon box reload (through saved configuration in the **show run** command), the existing licenses on the PEs is cleared and the PEs are monitored as usual for any future alarms.

The following information is cleared when you execute the **service-router service-monitor license-universal enable** command:

- Protocol Engine minor and major alarms

Note Alarm history commands continue to show all alarms as this is a different module.

- Protocol Engine internal vectors
- Protocol Engine alarm backup files in /tmp and /state

Burst Streaming License Control

Previously, the license limit was set to 500 Mbps and each protocol engine had a maximum number of sessions allowed. The base license limit is set to 200 sessions and 200 Mbps bandwidth.

When the number of sessions or current bandwidth usage exceeds the configured license limit on the Service Engine, the protocol engine raises an alarm and sends a `threshold exceeded` notification to the Service Router. Any new requests for that protocol engine are not routed to that Service Engine.

Note This feature only applies to the Windows Media Streaming engine.

Configure Burst Count

The protocol engines can trigger multiple minor alarms for session and bandwidth exceeded threshold conditions. If multiple minor alarms are triggered for a protocol engine in a single day (24-hour interval), they are recorded as a single alarm.

The burst count, which indicates the number of days after which a major alarm is raised, is configurable. On the Service Engine, use the service-router service-monitor threshold burstcnt command to configure the burst count. The default setting is one (1), which means all the minor alarms that occur in a single

day (24-hour interval) are counted as one single alarm. If the service-router service-monitor threshold burstcnt command is set to two, all minor alarms that occur in two days (48-hour interval) are counted as a single alarm.

Configure Universal License

A universal license is similar to a regular license, except it has a higher bandwidth and applies to all protocol engines (except Web Engine). When a universal license is purchased and configured, the alarm data for all protocol engines are cleared. Thereafter, the monitoring of the protocol engines continues as usual for any future alarms.

On the Service Engine, use the service-router service-monitor license-universal enable command to enable the universal license. The service-router service-monitor license-universal command is disabled by default.

Disk Failure Count Threshold

When the number of failed disks exceeds this threshold, no further requests are sent to this device and an alarm is raised. The Disk Failure Count Threshold is only for the CDNFS disks. Disk threshold configuration is the overall percentage of CDNFS disk failures after which an alarm is raised.

Note When an alarm is received for a SYSTEM disk, it is immediately marked as a failed disk. It is not checked against the Disk Failure Count Threshold. The SR continues redirecting to the SE, unless all SYSTEM disks on the SE are marked as failed disks

URL Translator

Use the **service-router lastresort domain** *domain* **translator** *ipaddress* command to configure the IP address of the third party URL translator. If a translator configuration is not present for any domain, it falls back to the alternate domain configuration. A maximum of one translator can be configured per content origin.

Service Router Transaction Log Fields

Table 2-9 describes the fields for the Service Router transaction log.

Table 2-9 Service Router Transaction Log Fields

Field	Description
c-ip	Source Internet Protocol (IP) address of the connected socket. This may be the IP address of a proxy server or firewall.
user-agent	Browser type used if the player was embedded in a browser. If the player was not embedded, this field refers to the user agent of the client that generated the log.
date	Date, in international date format, when a client is connected.
time	Time when the client is connected. The time format is either in Coordinated Universal Time (UTC) or local time, depending on how the logging plug-in is configured.
url	URL requested by the client.
protocol	Protocol used to access the content.
server-picked	Service Engine selected by the Service Router.
status	Status code.

Table 2-9 Service Router Transaction Log Fields (continued)

Field	Description
routing-method	Routing method chosen. The routing-method field has the following possible values: • Last-Resort • Network • Proximity • Zero-Network
routed-path	Request URL to redirect the client to a different CDN.

Service Monitor Transaction Logs

Service Monitor transaction logs provide an additional tool for analyzing the health history of a device and the protocol engines.

The device and service health information are periodically logged on the device in transaction log files. Transaction logs provide a useful mechanism to monitor and debug the system. The transaction log fields include both device and protocol engine information applicable to Service Engines and Service Routers that are useful for capacity monitoring. Additionally, when a device or protocol engine threshold is exceeded, detailed information is sent to a file (threshold_exceeded.log) to capture the processes that triggered the threshold alarm.

The Service Monitor transaction log filename has the following format: service_monitor_<*ipaddr*>_*yyyymmdd_hhmmss*_<>, where:

- <*ipaddr*> represents the IP address of the SE, SR, or VOSM.
- *yyyymmdd_hhmmss* represents the date and time when the log was created.

For example, service_monitor_192.168.1.52_20110630_230001_00336 is the filename for the log file on the device with the IP address of 192.168.1.52 and a time stamp of June 30, 2011 at 3:36 AM.

The Service Monitor transaction log file is located in the /local1/logs/service_monitor directory.

An entry to the Service Monitor transaction log is made every two seconds.

Note The following rules apply to Service Monitor transaction logs:

- A transaction log value is only logged if the Service Monitor is enabled for that component or protocol engine on the device. For example, if CPU monitoring is not enabled, the transaction log value "–" is displayed.
- If Service Monitor is enabled for a protocol engine, but the protocol engine is not enabled, the value is not displayed in the log file.
- If a log field can have more than one value, the values are delimited by the pipe (|) character.
- If a value can have sub-values, the sub-values are delimited by the carrot (^) character.
- Some of the fields display aggregate values. If the statistics are cleared using the clear statistics command, the value after clearing the statistics may be less than the previous values, or may be zero (0).

Table 2-10 describes the fields for the Service Monitor transaction log on an SE.

Table 2-10 SE Service Monitor Transaction Log Fields

Field	Sample Output	Description	Corresponding CLI Command
date	2011-06-30	Date of log.	–
time	22:52:02	Time of log.	–
cpu_avg	21	Moving average value in percentage of CPU usage.	show service-router service-monitor Device status—CPU—Average load
mem_avg	44	Moving average value in percentage of memory usage.	show service-router service-monitor Device status—Mem—Average used memory
kernel_mem_avg	11	Moving average value in percentage of kernel memory.	show service-router service-monitor Device status—KMEM—Average kernel memory
disk_avg	2	Moving average value in percentage of disk usage.	show service-router service-monitor Device status—Disk—Average load
disk_fail_count_ threshold	Y	Boolean value to indicate if disk fail count threshold has been reached.	show service-router service-monitor Device status—Device Status—Disk—Status
per_disk_load	disk03-01^2| disk04-02^5	Current load per disk, as a percentage. The sample output indicates that disk03–partition01 has a 2 percent load and disk04–partition02 have a 5 percent load.	–
bandwidth_avg	Port_Channel_ 1^2^4| Port_Channel_ 2^0^0	Moving average bandwidth used, as a percentage, of bandwidth in and bandwidth out per interface. The sample output indicates that port channel 1 has an average bandwidth of 2 percent for receiving and 4 percent for transmitting, and port channel 2 average bandwidth usage is 0.	**show service-router service-monitor** Device status—NIC—Average BW In/ Average BW Out
file_desc_count	1023	Total count of file descriptors open on the device. File descriptors are internal data structures maintained by the Linux kernel for each open file.	–
tcp_server_connections	35	Number of TCP server connections open.	**show statistics tcp** TCP Statistics—Server connection openings
tcp_client_connections	24	Number of TCP client connections open.	**show statistics tcp** TCP Statistics—Client connection openings
processes_count	42	Number of processes running on the device.	**show processes**
dataserver_cpu_ percentage	1	Percentage of the CPU used for the dataserver process.	–

Table 2-10 SE Service Monitor Transaction Log Fields (continued)

Field	Sample Output	Description	Corresponding CLI Command
web_ engine_ threshold_exceeded	Y	Boolean value to indicate if the Web Engine threshold has been exceeded.	**show service-router service-monitor** Services status—Web—Threshold
web_ engine_augment_ threshold_exceeded	Y	Boolean value to indicate if Web Engine augmentation alarm threshold has been exceeded.	–
web_ engine_stopped	N	Boolean value to indicate if Web Engine has stopped.	**show service-router service-monitor** Services status—Web—Stopped
web_engine_cpu_ percentage	3	Percentage of the CPU used by the Web Engine.	–
web_engine_mem (bytes)	3500	Memory (in bytes) used by the Web Engine.	**show web-engine health** Total memory usage
web_engine_get_ requests	250	Count of get requests received by the Web Engine (Aggregate value)	**show statistics web-engine detail** HTTP Request Type Statistics—Get requests
web_engine_sessions	5	Count of HTTP connections.	**show statistics web-engine detail** Web Engine Detail Statistics—Total HTTP Connection + Active Session
web_engine_upstream_ connections	2	Count of HTTP connections to upstream SE or origin service.	**show statistics web-engine detail** Web Engine Detail Statistics—Total HTTP Connection
rtspg_tps	12	Current RTSP Gateway transactions per second (TPS).	–
uns_cpu_percentage	3	Percentage of CPU used by the Unified Namespace (UNS) process.	–
uns_mem (bytes)	3500	Memory used by the UNS process.	–

Table 2-11 describes the fields for the Service Monitor transaction log on a SR.

Table 2-11 SR Service Monitor Transaction Log Fields

Field	Sample Output	Description	Corresponding CLI Command
date	2011-06-30	Date of log.	–
time	22:52:02	Time of log.	–
cpu_avg	21	Moving average value in percentage of CPU usage.	**show service-router service-monitor Device status**—CPU—Average load
mem_avg	44	Moving average value in percentage of memory usage.	**show service-router service-monitor Device status**—Mem—Average used memory
kernel_mem_avg	11	Moving average value in percentage of kernel memory.	**show service-router service-monitor** Device status—KMEM—Average kernel memory
disk_avg	2	Moving average value in percentage of disk usage.	**show service-router service-monitor** Device status—Disk—Average load

Table 2-11 SR Service Monitor Transaction Log Fields (continued)

Field	Sample Output	Description	Corresponding CLI Command
disk_fail_count_ threshold	Y	Boolean value to indicate if disk fail count threshold has been reached.	**show service-router service-monitor** Device status—Device Status—Disk—Status
file_desc_count	1023	Total count of file descriptors open on the device. File descriptors are internal data structures maintained by the Linux kernel for each open file.	–
tcp_server_connections	35	Number of TCP server connections open.	**show statistics tcp** TCP Statistics—Server connection openings
tcp_client_connections	24	Number of TCP client connections open.	**show statistics tcp** TCP Statistics—Client connection openings
processes_count	42	Number of processes running on the device.	**show processes**
dataserver_cpu_ percentage	1	Percentage of the CPU used for the dataserver process.	–
sr_cpu_percentage	12	Cpu percentage used by SR.	–
sr_mem (bytes)	750000	Memory (in bytes) used by SR.	**show processes memory** and search for service_router
requests_received	34	Total count of requests received by SR (aggregate value)	**show statistics service-router summary** Requests Received
http_normal_requests_ received	5	Total count of normal HTTP requests received by SR (aggregate value).	**show statistics service-router summary** HTTP Requests (normal)
http_asx_requests_ received	5	Total count of ASX HTTP requests received by SR (aggregate value).	**show statistics service-router summary**- HTTP Requests (ASX)
rtsp_requests_received	5	Total count of RTSP requests received by SR (aggregate value).	**show statistics service-router summary** RTSP Requests
rtmp_requests_received	5	Total count of RTMP requests received by SR (aggregate value).	**show statistics service-router summary** RTMP Requests
dns_requests_received	6	Total count of Domain Name System (DNS) requests received by SR (aggregate value).	**show statistics service-router dns** Total DNS queries

Examples

The following example shows how to configure the keepalive interval:

```
ServiceRouter(config)# service-router keepalive-interval 2
```

The following example shows how to configure the service monitor type:

```
ServiceRouter(config)# service-router service-monitor type all
```

Augmentation Alarms

The augmentation alarms threshold is a percentage, that applies to the CPU, memory, kernel memory, disk, disk fail count, Network Information Center (NIC), and protocol engine usages. By default it is set to 80 percent.

As an example of an augmentation alarm, if the threshold configured for CPU usage is 80 percent, and the augmentation threshold is set to 80 percent, then the augmentation alarm for CPU usage is raised when the CPU usage crosses 64 percent.

If “A” represents the Service Monitor threshold configured, and “B” represents the augmentation threshold configured, then the threshold for raising an augmentation alarm = (A * B) / 100 percent.

The threshold value range is 1–100. The following command shows how to set the augmentation alarms threshold to 70 percent:

```
ServiceRouter(config)# service router service-monitor threshold augmentation 70
```

The following command shows how to reset the augmentation alarm threshold to the default:

```
ServiceRouter(config)# no service router service-monitor threshold augmentation 70
```

The **show service-router service monitor** command displays the augmentation alarm threshold configuration.

The **show alarms** command displays the alarms output.

The **show alarms history detail** command displays the history details.

The **show alarms detail** command displays the alarms details.

The **show alarms detail support** command displays the support information.

Cross Domain Support

The following example shows how to configure the failed disk threshold to 40 percent:

```
ServiceEngine(config)# service-router service-monitor threshold faildisk 40
U2-205-2(config)#end
U2-205-2#show running-config | include threshold
service-router service-monitor threshold faildisk 40
ServiceEngine#
```

To display the statistics, use the **show statistics service-router summary** command and the **show statistics se** *sename* command. The new output for the DNS-Based Redirection feature is highlighted in boldface type in the examples below. In addition to these two **show** commands, there is also the **show statistics service-router dns** command, which displays the same output as before:

```
ServiceRouter# show statistics service-router summary

----- SR Summary Statistics -----

Requests Received        :               650
  HTTP Requests (normal) :               650
  HTTP Requests (API)    :                 0
  DNS Requests           :                 0

Requests Served          :                 0
  HTTP Requests Served   :                 0

Requests Redirected      :               650
  HTTP 302 Redirects     :               650
  HTTP API Redirects     :                 0
```

```
  DNS redirects          :                  0

Requests Overflowed      :                  0
  HTTP 302 Redirects     :                  0
  HTTP API Redirects     :                  0
  DNS redirects          :                  0

Requests Not Redirected  :                  0
  No SE Covering Client  :                  0
  Unknown Content Origin :                  0
  Invalid Requests       :                  0

  "Stale SE" Requests    :                  0

ServiceRouter# show statistics service-router se temp2

----- Statistics Of SE: temp2 -----
IP Address              : 2.225.2.59
Aliveness               : up
HTTP 302 Redirects      :                  0
ASX Redirects           :                  0
RTSP Redirects          :                  0
RTMP Redirects          :                  0
DNS Redirects           :                  1
Number Of Keepalives    :              85261
```

The following example shows how to enable the Service Monitor transaction logging:

```
ServiceEngine(config)# transaction-logs enable
ServiceEngine(config)# service-router service-monitor transaction-log enable
```

The following example shows how to configure the URL translator:

```
ServiceRouter(config)# service-router last-resort domain vos.com translator 171.XX.XX.XXX
ServiceRouter(config)# service-router last-resort domain vosis.com translator
171.XX.XX.XXX port 8080
ServiceRouter#
```

The following example shows how to verify the current last resort configuration details:

```
ServiceRouter# show service-router last-resort
Domain vos.com translator 171.XX.XX.XXX
Domain vosis.com translator 171.XX.XX.XXX port 8080
```

Related Commands

Command	Description
show service-router	Displays the Service Router configuration.

setup

To configure basic configuration settings (general settings, device network settings, and disk configuration) on the SE and a set of commonly used caching services, use the **setup** command in EXEC configuration mode. You can also use the **setup** command in EXEC configuration mode to complete basic configuration after upgrading.

setup

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **setup** command is not supported for virtual machines (VMs). Instead, use the instructions for deploying a VM in the *Cisco Videoscape Distribution Suite Origin Server Command Reference*.

Examples

The following example shows the part of the output when you enter the **setup** command in EXEC configuration mode on an SE running the VDS-OS software:

```
ServiceEngine# setup

Here is the current profile of this device

CDN device                    : Yes

Do you want to change this (y/n) [ n ] :


Press the ESC key at any time to quit this session
```

show access-lists

To display the access control list (ACL) configuration, use the **show access-lists** command in EXEC configuration mode.

show access-lists

Syntax Description

This command has no arguments or keywords**.**

Command Default

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-12 describes the fields shown in the **show access-lists 300** display.

Table 2-12 show access-lists Field Descriptions

Field	Description
Access Control List is enabled	Configuration status of the access control list.
Groupname and username-based List	Lists the group name-based access control lists.

Related Commands

Command	Description
access-lists	Configures access control list entries.

show alarms

To display information on various types of alarms, their status, and history, use the **show alarms** command in EXEC configuration mode.

show alarms [**critical** [**detail** [**support**] | **detail** [**support**] | **history** [*start_num* [*end_num* [**detail** [**support**] | **detail** [**support**]]] | **critical** [*start_num* [*end_num* [**detail** [**support**]] | **detail** [**support**]]] | **detail** [**support**] | **major** [*start_num* [*end_num* [**detail** [**support**]] | **detail** [**support**]]] | **minor** [*start_num* [*end_num* [**detail** [**support**]]] | **detail** [**support**]]] | **major** [**detail** [**support**]] | **minor** [**detail** [**support**]]] | **status**]]

Syntax Description

critical	(Optional) Displays critical alarm information.
detail	(Optional) Displays detailed information for each alarm.
support	(Optional) Displays additional information about each alarm.
history	(Optional) Displays information about the history of various alarms.
start_num	(Optional) Alarm number that appears first in the alarm history (1 to 100).
end_num	(Optional) Alarm number that appears last in the alarm history (1 to 100).
major	(Optional) Displays information about major alarms.
minor	(Optional) Displays information about minor alarms.
status	(Optional) Displays the status of various alarms and alarm overload settings.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The Node Health Manager enables VDS-OS applications to raise alarms to draw attention to error or significant conditions. The Node Health Manager, which is the data repository for such alarms, aggregates the health and alarm information for the applications, services (for example, the cache service), and resources (for example, disk drives) that are being monitored on the SE. For example, the Node Health Manager gives you a mechanism to determine if a monitored application (for example, the HTTP proxy caching service) is alive on the SE. These alarms are referred to as VDS-OS software alarms.

The VDS-OS software uses Simple Network Management Protocol (SNMP) to report error conditions by generating SNMP traps. In the VDS-OS software, the following SE applications can generate a VDS-OS software alarm:

- Node Health Manager (alarm overload condition and Node Manager aliveness)
- Node Manager for service failures (aliveness of monitored applications)
- System Monitor (sysmon) for disk failures

The three levels of alarms in the VDS-OS software are as follows:

- Critical—Alarms that affect the existing traffic through the SE and are considered fatal (the SE cannot recover and continue to process traffic).

- Major—Alarms that indicate a major service (for example, the cache service) has been damaged or lost. Urgent action is necessary to restore this service. However, other node components are fully functional and the existing service should be minimally impacted.
- Minor—Alarms that indicate that a condition that will not affect a service has occurred, but corrective action is required to prevent a serious fault from occurring.

You can configure alarms using the **snmp-server enable traps alarm** command in global configuration mode.

Use the **show alarms critical** command in EXEC configuration mode to display the current critical alarms being generated by the VDS-OS software applications. Use the **show alarms critical detail** command in EXEC configuration mode to display additional details for each of the critical alarms being generated. Use the **show alarms critical detail support** command in EXEC configuration mode to display an explanation about the condition that triggered the alarm and how you can find out the cause of the problem. Similarly, you can use the **show alarms major** and **show alarms minor** command in EXEC configuration modes to display the details of major and minor alarms.

Use the **show alarms history** command in EXEC configuration mode to display a history of alarms that have been raised and cleared by the VDS-OS software on the SE. The VDS-OS software retains the last 100 alarm raise and clear events only.

Use the **show alarm status** command in EXEC configuration mode to display the status of current alarms and the SE's alarm overload status and alarm overload configuration.

Note The maximum concurrent sessions limit for the Web Engine is based on the CDE; for the CDE220-2M0 and CDE220-2S6 the maximum is 30,000 and for the CDE205 the maximum is 20,000.

Brstcnt Threshold Alarm

When the number of sessions or current bandwidth usage exceeds the configured license limit on the Service Engine, the protocol engine raises an alarm and sends a `threshold exceeded` notification to the Service Router. Any new requests for that protocol engine are not routed to that Service Engine.

Note This feature only applies to the Windows Media Streaming engine.

Table 2-13 describes the fields shown in the **show alarms history** display.

Table 2-13 show alarms history Field Descriptions

Field	Description
Op	Operation status of the alarm. Values are R—Raised or C—Cleared.
Sev	Severity of the alarm. Values are Cr—Critical, Ma—Major, or Mi—Minor.
Alarm ID	Type of event that caused the alarm.
Module/Submodule	Software module affected.
Instance	Object that this alarm event is associated with. For example, for an alarm event with the Alarm ID disk_failed, the instance would be the name of the disk that failed. The Instance field does not have pre-defined values and is application specific.

Table 2-14 describes the fields shown in the **show alarms status** display.

Table 2-14 show alarms status Field Descriptions

Field	Description
Critical Alarms	Number of critical alarms.
Major Alarms	Number of major alarms.
Minor Alarms	Number of minor alarms.
Overall Alarm Status	Aggregate status of alarms.
Device is NOT in alarm overload state.	Status of the device alarm overload state.
Device enters alarm overload state @ 999 alarms/sec.	Threshold number of alarms per second at which the device enters the alarm overload state.
Device exits alarm overload state @ 99 alarms/sec.	Threshold number of alarms per second at which the device exits the alarm overload state.
Overload detection is enabled.	Status of whether overload detection is enabled on the device.

Related Commands

Command	Description
alarm	Configure alarms.
snmp-server enable traps	Enables the Service Engine (SE) to send Simple Network Management Protocol (SNMP) traps.

show arp

To display the Address Resolution Protocol (ARP) table, use the **show arp** command in EXEC configuration mode.

show arp

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **show arp** command displays the Internet-to-Ethernet address translation tables of the ARP. Without flags, the current ARP entry for the hostname is displayed.

Table 2-15 describes the fields shown in the **show arp** display.

Table 2-15 show arp Field Descriptions

Field	Description
Protocol	Type of protocol.
Address	Ethernet address of the hostname.
Flags	Current ARP flag status.
Hardware Addr	Hardware Ethernet address given as six hexadecimal bytes separated by colons.
Type	Type of wide area network.
Interface	Type of Ethernet interface.

show authentication

To display the authentication configuration, use the **show authentication** command in EXEC configuration mode.

show authentication user

Syntax Description

user	Displays the authentication configuration for the user login to the system.

Defaults

None

Command Modes

EXEC configuration mode.

Related Commands

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.

show banner

To display information on various types of banners, use the **show banner** command in EXEC configuration mode.

show banner

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-16 describes the fields shown in the **show banner** display.

Table 2-16 show banner Field Descriptions

Field	Description
Banner is enabled.	Configuration status of the banner feature.
MOTD banner is: abc	Displays the configured message of the day (MOTD).
Login banner is: acb	Displays the configured login banner.
Exec banner is: abc	Displays the configured EXEC banner.

Related Commands

Command	Description
banner	Configures the EXEC, login, and message-of-the-day (MOTD) banners.

show cdnfs

To display CDS network file system (CDNFS) information, use the **show cdnfs** command in EXEC configuration mode.

show cdnfs {**usage** | **volumes**}

Syntax Description

usage	Displays Content Delivery Network (CDN) current usage.
volumes	Displays VDS-OS NFS volumes.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

If there are any **clear cache all** commands in progress, the **show cdnfs usage** command displays the progress. If any disks are marked for not creation, then the disk is listed here and the reason is provided.

Table 2-17 describes the fields shown in the **show cdnfs volumes** display.

Table 2-17 show cdnfs volumes Field Descriptions

Field	Description
cdnfs 00–04	CDS network file system and disk number.
nnnnnnKB	Size of the volume in kilobytes.

Table 2-18 describes the fields shown in the **show cdnfs usage** display.

Table 2-18 show cdnfs usage Field Descriptions

Field	Description
Total number of CDNFS entries	Shows the total number of CDNFS entries.
Total space	Shows the total disk space.
Total bytes available	Shows the available disk space.
Total cache size	Shows the total cache size
Total cached entries	Shows the total cache and preposition entries.
Cache-content mgr status	Shows the current status of whether or not the Content Manager is cacheable.

Examples

The following example shows how to display the CDNFS usage on an SE:

```
ServiceEngine# show cdnfs usage
Total number of CDNFS entries  :   13437532
Total space                    :     5037.9 GB
Total bytes available          :     2425.6 GB
Total cache size               :     2521.4 GB
Total cached entries           :   13436995
Cache-content mgr status       :        Cacheable
 Units: 1KB = 1024B; 1MB = 1024KB; 1GB = 1024MB
```

The following example shows how to display the CDNFS volumes:

```
ServiceEngine# show cdnfs volumes
cdnfs 00: /disk00-06          444200480KB
cdnfs 01: /disk01-06          444200480KB
cdnfs 02: /disk03-01          488246296KB
cdnfs 03: /disk04-01          488247316KB
cdnfs 04: /disk05-01          488246296KB
cdnfs 05: /disk06-01          488244924KB
cdnfs 06: /disk07-01          488244924KB
cdnfs 07: /disk09-01          488244924KB
cdnfs 08: /disk10-01          488244924KB
cdnfs 09: /disk11-01          488246296KB
cdnfs 10: /disk08-01          488377368KB
```

Related Commands

Command	Description
cdnfs	Manages the CDS network file system (cdnfs).
disk (EXEC)	Configures disks and allocates disk space for devices that are using the VDS-OS software.
show disks	Displays the names of the disks currently attached to the SE.
show statistics cdnfs	Displays SE CDS network file system (cdnfs) statistics.

show clock

To display the system clock, use the **show clock** command in EXEC configuration mode.

show clock [**detail | standard-timezones** {**all | details** *timezone* | **regions | zones** *region_name*}]

Syntax Description

detail	(Optional) Displays detailed information; indicates the Network Timing Protocol (NTP) clock source and the current summer time setting (if any).
standard-timezones	(Optional) Displays information about the standard time zones.
all	Displays all the standard time zones (approximately 1500 time zones). Each time zone is listed on a separate line.
details	Displays detailed information for the specified time zone.
timezone	Name of the time zone.
regions	Displays the region name of all the standard time zones. All 1500 time zones are organized into directories by region.
zones	Displays the name of every time zone that is within the specified region.
region_name	Name of the region.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The VDS-OS has several predefined standard time zones. Some of these time zones have built-in summertime information while others do not. For example, if you are in an eastern region of the United States (US), you must use the US/Eastern time zone that includes summertime information and adjusts the clock automatically every April and October. There are about 1500 standard time zone names.

The **clock summertime** command is disabled when a standard time zone is configured. You can only configure summertime if the time zone is not a standard time zone (if the time zone is a customized zone).

In addition, CLI commands exist to enable you to display a list of all the standard time zones. The **show clock standard-timezones all** command in EXEC configuration mode enables you to browse through all standard time zones and choose from these predefined time zones. You can choose a customized name that does not conflict with the predefined names of the standard time zones. Most predefined names of the standard time zones have two components, a region name and a zone name. You can list time zones by several criteria, such as regions and zones.

Table 2-19 describes the field in the **show clock** display.

Table 2-19 show clock Field Description

Field	Description
Local time	Day of the week, month, date, time (hh:mm:ss), and year in local time relative to the Coordinated Universal Time (UTC) offset.

Table 2-20 describes the fields shown in the **show clock detail** display.

Table 2-20 show clock detail Field Descriptions

Field	Description
Local time	Local time relative to UTC.
UTC time	UTC date and time.
Epoch	Number of seconds since Jan. 1, 1970.
UTC offset	UTC offset, in seconds, hours, and minutes.

The following example shows an excerpt of the output from the **show clock standard-timezones all** command in EXEC configuration mode. As the following example shows all the standard time zones (approximately 1500 time zones) are listed. Each time zone is listed on a separate line.

```
ServiceEngine #  show clock standard-timezones all
Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
Africa/Algiers
Africa/Asmera
Africa/Bamako
Africa/Bangui
Africa/Banjul
Africa/Bissau
Africa/Blantyre
Africa/Brazzaville
Africa/Bujumbura
Africa/Casablanca
Africa/Ceuta
Africa/Conakry
Africa/Dakar
Africa/Dar_es_Salaam
Africa/Djibouti
.
.
.
```

The following example shows an excerpt of the output from the **show clock standard-timezones region** command in EXEC configuration mode. As the example shows, all first level time zone names or directories are listed. All 1500 time zones are organized into directories by region.

```
ServiceEngine #  show clock standard-timezones regions
Africa/
America/
Antarctica/
Arctic/
Asia/
Atlantic/
Australia/
Brazil/
CET
.
.
.
```

The following example shows an excerpt of the output from the **show clock standard-timezones zones** command in EXEC configuration mode. As the following example shows, this command lists the name of every time zone that is within the specified region (for example, the US region).

```
ServiceEngine# show clock standard-timezones zones US
Alaska
Aleutian
Arizona
Central
East-Indiana
Eastern
Hawaii
Indiana-Starke
Michigan
Mountain
Pacific
Samoa
```

The following example shows an excerpt of the output from the **show clock standard-timezones details** command in EXEC configuration mode. This command shows details about the specified time zone (for example, the US/Eastern time zone). The command output also includes the standard offset from the Greenwich Mean Time (GMT).

```
ServiceEngine # show clock standard-timezones details US/Eastern
US/Eastern is standard timezone.
Getting offset information (may take a while)...
Standard offset from GMT is -300 minutes (-5 hour(s)).
It has built-in summertime.
Summer offset from GMT is -240 minutes. (-4 hour(s)).
```

Related Commands

Command	Description
clock (EXEC)	Sets or clears clock functions or updates the calendar.
clock (global configuration	Sets the summer daylight saving time and time zone for display purposes.

show cms

To display the Centralized Management System (CMS)-embedded database content and maintenance status and other information, use the **show cms** command in EXEC configuration mode.

show cms {**database** {**content** {**dump** *filename* | **text** | **xml**} | **maintenance** [**detail**]} | **info** | **processes**}

Syntax Description

database	Displays embedded database maintenance information.
content	Writes the database content to a file.
dump	Dumps all database content to a text file.
filename	Name of the file to be saved under local1 directory.
text	Writes the database content to a file in text format.
xml	Writes the database content to a file in Extensible Markup Language (XML) format.
maintenance	Shows the current database maintenance status.
detail	(Optional) Displays database maintenance details and errors.
info	Displays CMS application information.
processes	Displays CMS application processes.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-21 describes the fields shown in the VOSM **show cms info** display.

Table 2-21 show cms Field Descriptions for the VOSM

Field	Description
CDN information	
Model	Model name of the device.
Node Id	Unique identifier given to the device by the VOSM at registration, which is used to manage the device.
Device Mode	Configured mode of device used during registration.
Current VOSM role	Role of the current VOSM: Primary or Standby.
CMS services information	
Service cms_httpd is running	Status of the cms_httpd management service (running or not running). This field is specific to the VOSM only.
Service cms_VOSM is running	Status of the cms_VOSM management service (running or not running). This field is specific to the VOSM only.

Table 2-22 describes the fields shown in the SE **show cms info** display.

Table 2-22 show cms Field Descriptions for the SE

Field	Description
CDN information	
Model	Model name of the device.
Node Id	Unique identifier given to the device by the VOSM at registration, which is used to manage the device.
Device Mode	Configured mode of device used during registration.
Current VOSM address	Address of the VOSM as currently configured in the **vosm ip** command in global configuration mode. This address may differ from the registered address if a standby VOSM is managing the device instead of the primary VOSM with which the device is registered.
Registered with VOSM	Address of the VOSM with which the device is registered.
Status	Connection status of the device to the VOSM. This field may contain one of three values: Online, Offline, or Pending.
Time of last config-sync	Time when the device management service last contacted the VOSM for updates.

The following example writes the database content to a file in text format:

```
VOSM# show cms database content text
Database content can be found in /local1/cms-db-12-12-2002-17:06:08:070.txt.
```

The following example writes the database content to a file in XML format:

```
VOSM# show cms database content xml
Database content can be found in /local1/cms-db-12-12-2002-17:07:11:629.xml.
```

The following example shows the output of the **show cms database maintenance detail** on an SE:

```
ServiceEngine# show cms database maintenance detail
Database maintenance is not running.
Regular database maintenance is enabled.
Regular database maintenance schedule is set on Sun, Mon, Tue, Wed, Thu, Fri, Sat at 02:00
Full database maintenance is enabled.
Full database maintenance schedule is set on Sun, Mon, Tue, Wed, Thu, Fri, Sat at 04:00
Disk usage for STATE partition: Total: 1523564K, Available: 1443940K, Use: 6%

DATABASE VACUUMING DETAILS AND ERRORS
-------------------------------------
Database Vacuuming never performed or it did not complete due to error.
Latest Vacuuming status :No Error
Last Vacuum Error : No Error
Last Reindex Time : Thu Jul 15 02:02:49 2004
Latest Reindexing status :No Error
Last Reindex Error: No Error
ServiceEngine#
```

Related Commands

Command	Description
cms (EXEC)	Configures the CMS-embedded database parameters.
cms (global)	Schedules maintenance and enables the CMS on a given node.

show content

To display all content entries in the VDS-OS, use the **show content** command in EXEC configuration mode.

show content {**all** [**brief** | **foreground**] | **diskpath** [**brief** | **detail**] | **last-folder-url** [**brief**] | **url** *url* [**brief** | **detail**]}

Syntax Description

all	Displays all cached content into a file.
name	Output file to log cache content query results.
brief	(Optional) Indicates that this brief display mode should be used.
foreground	(Optional) Indicates that this command should be run in the foreground.
diskpath	Displays cached content objects with the original diskpath.
detail	(Optional) Indicates that the detail display mode should be used.
last-folder-url	Displays all content with relative diskpath from the given url without a filename.
url	Displays the cached content object with original URL.
url	The original URL for cache content object query.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **show content** command is not supported in VDS-OS 2.0.

This command allows users to check the cached or prepositioned content in an SE. Through this command, users can view content attributes such as status and file size.

The **show content all** command scans through the entire disk and transfers the information to the file specified by the user. This command runs in the background unless the foreground option is specified.

The **show content url** command displays cached content and Web Engine metadata attributes, and it helps debug header validation issues. It also displays additional information including start, end time, unified name space (UNS), and relative content information. If the input URL is parent, then it shows the child disk path. The Authorization field is only applicable for preposition content and this field is moved to the **show content url detail** output.

When executing the **show content url** command with live URL, it displays as preposition content. This is because the object stored on CDS network file system (CDNFS) is either cache content or preposition content.

Examples

The following command shows how to display cached content and Web Engine attributes for a URL:

```
ServiceEngine# show content url http://172.XX.XX.XXX/diff.new detail

CAL content object attributes:
```

```
        URL: http://we-os.vos.com/vod/pinball.wmv
        Status is 3 (Servable)
        Content is Complete
        File size is 0 Bytes
        Linked to
[rtsp://http-we-os.vos.com-s6kmyz359zgyulqfiavhgw/vod/pinball.wmv]
        Content is PREPOSITIONED
        Start Time : Not present
        End Time : Not present
        Internal path to data file
[/disk00-06/p/we-os.vos.com/1d/a1/1da1394af838bbcb45af78fd5681abeb/pinball.w
mv]

Protocol Engine Metadata:
        Authorization is Not Required
        uns_attr_symlink :
http-we-os.vos.com-s6kmyz359zgyulqfiavhgw/vod/pinball.wmv
        UNS_NV_CALC_N_CACHED : PREPOSITIONED
        cdn_uns_id : Rm+7u02g2S8PsuaCfnOKAQ. .
        content-type : video/x-ms-wmv
        etag : "9601c7-cc3d0-11016c00"
        file_duration : 25
        ignore_query_string : 1
        last-modified : Wed, 06 Oct 2010 22:12:00 GMT
        server : Apache/2.2.3 (Red Hat)
```

The following example shows how to display the Real-Time Streaming Protocol (RTSP) URL in the VDS-OS:

```
ServiceEngine# show content url rtsp://www.cht.com/CHT_2M.wmv
CAL content object attributes:
URL: rtsp://www.cht.com/CHT_2M.wmv
Status is 2 (Servable)
File size is 16 Bytes
Authorization is Not Required
Content is CACHED with priority 0.574964
```

The following example shows how to display all content entries in the VDS-OS:

```
ServiceEngine# show content all name background
Command running in background...
ServiceEngine# USER INFO: Your 'show content all' command finished
```

The following example shows how to display cached content objects with the original diskpath.

```
ServiceEngine# show content diskpath
/disk02-01/c/171.71.51.234/66/66/6666cd76f96956469e7be39d750cc7d9/1mbs.wmv.hdr

CAL content object attributes:
        URL: rtsp://171.XX.XX.XXX/1mbs.wmv.hdr
        Status is 3 (Servable)
        Content is Incomplete
        File size is 4096 Bytes
        Authorization is Not Required
        Content is CACHED with priority 0.303707
```

The following example shows how to display all the contents matching to that last-folder-url with the brief option:

```
ServiceEngine# show content last-folder-url http://172.XX.XX.XXX/vod/types brief
Protocol will be ignored with last-folder-url.
-----------------------------------------------------------------
Type URL                                        Size(K)   Status
-----------------------------------------------------------------
```

```
C    http://172.XX.XX.XXX/vod/types/sample_s  81        Servable
     orenson.mov
C    http://172.XX.XX.XXX/vod/types/sample_1  912       Servable
     00kbit.mp4
C    http://172.XX.XX.XXX/vod/types/brodeo.m  3745      Servable
     p3
```

The following example shows how to display all the contents matching to that last-folder-url without the brief option:

```
ServiceEngine# show content last-folder-url http://172.XX.XX.XXX/vod/types
Protocol will be ignored with last-folder-url.

CAL content object attributes:
        URL: http://172.XX.XX.XXX/vod/types/sample_sorenson.mov
        Status is 3 (Servable)
        Content is Complete
        File size is 82395 Bytes
        Playable by Web Engine
        Content is CACHED

CAL content object attributes:
        URL: http://172.XX.XX.XXX/vod/types/sample_100kbit.mp4
        Status is 3 (Servable)
        Content is Complete
        File size is 933456 Bytes
        Playable by Web Engine
        Content is CACHED

CAL content object attributes:
        URL: http://172.XX.XX.XXX/vod/types/brodeo.mp3
        Status is 3 (Servable)
        Content is Complete
        File size is 3834862 Bytes
        Playable by Web Engine
        Content is CACHED
```

show content-origin

To display information about the Network-Attached Storage (NAS) mount, use the **show content-origin** command in user EXEC configuration mode.

show content-origin request-fqdn *domain*

Syntax Description

request-fqdn	Configures the request fully qualified domain name (FQDN).
domain	Domain of the request FQDN.

Command Default

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

Table 2-22 describes the fields shown in the **show content-origin** display.

Table 2-23 show content-origin Field Descriptions

Field	Description
FQDN	Fully Qualified Domain Name of the content origin.
Protocol	Protocol used.
SharePoint	SharePoint IP address.
MountPoint	MountPoint type.
Status	Indicates if it succeeded or failed.
MaxRetry	Maximum number of retries allowed.
RetryCount	Actual number of retries.

The following syslog messages are displayed if the NAS mount fails:

```
Vos Origin Manager writes syslog messages when NAS mount fails. Below are some sample
syslog messages:
Apr 28 04:25:26 nas-se VOSOriginMgr: %SE-VOSOriginMgr-3-802100: Failed to mount NFS vod/0
for NAS share 14.1.2.12:/ifs/data
```

Examples

The following example shows how to display the content origin information:

```
ServiceEngine# show content-origin
FQDN: www.cisco.com
      Protocol: CIFS
      SharePoint: 171.XX.XX.X:/wmroot
      MountPoint: WMS
      Status: Success

      Protocol: NFS
      SharePoint: 171.XX.XX.XXX:/usr/local/apache2/htdocs/Zeri
```

```
MountPoint: ZERI
Status: Failed
MaxRetry: 10
RetryCount: 17
ServiceEngine#
```

Related Commands

Command	Description
content-origin	Supports multiple origin services within a content origin.

show debugging

To display the state of each debugging option, use the **show debugging** user command in user EXEC configuration mode.

show debugging

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

User EXEC configuration mode.

Examples

The following is sample output from the **show debugging** command:

```
ServiceRouter# show debugging
Debug web-engine is set to trace
Debug capturecontroller is set to trace
ServiceRouter#
```

Related Commands

Command	Description
debug	Monitors and records caching application functions.
undebug	Disables debugging functions.

show device-mode

To display the configured or current mode of a device, use the **show device-mode** command in EXEC configuration mode.

show device-mode {**configured** | **current**}

Syntax Description

configured	Displays the configured device mode.
current	Displays the current device mode.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

If the configured and current device modes differ, a reload is required for the configured device mode to take effect.

Examples

The configured device mode field in the **show device-mode configured** display shows the device mode that has been configured, but has not yet taken effect. The current device mode field in the **show device-mode current** command display shows the current mode in which the VDS-OS device is operating.

The following example shows how to use the **show device-mode** command to show the device mode when you change the device from an SE to an SR using the **device mode** command:

```
Acmehost# show device-mode current
Current device mode: service-engine
Acmehost# show device-mode configured
Configured device mode: service-engine
Acmehost(config)# device mode service-router
The new configuration will take effect after a reload
Acmehost(config)# exit
Acmehost# show device-mode current
Current device mode: service-engine
Note: The configured and current device modes differ,
a reload is required for the configured device mode to
take effect.
Acmehost# show device-mode configured
Configured device mode: service-router
Note: The configured and current device modes differ,
a reload is required for the configured device mode to
take effect.
Acmehost# write memory
Acmehost# reload force
...reload...


Acmehost# show running-config
device mode service-router
!
```

```
hostname Acmehost
. .

Acmehost# show device-mode configured
Configured device mode: service-router
Acmehost# show device-mode current
Current device mode: service-router
```

Related Commands

Command	Description
device	Configures the mode of operation on a device as a VOSM, SE or SR.

show disks

To view information about your disks, use the **show disks** command in EXEC configuration mode.

show disks [**current** | **details** | **error-handling** [**details**] | **raid-state** | **SMART-info** [**details**]]

Syntax Description

current	(Optional) Displays currently effective configurations.
details	(Optional) Displays currently effective configurations with more details.
error-handling	(Optional) Displays the disk error-handling statistics.
details	(Optional) Displays the detail disk and sector errors.
raid-state	(Optional) Displays the volume and progress information for the RAID disks.
SMART-info	(Optional) Displays hard drive diagnostic information and information about impending disk failures.
details	(Optional) Displays Self Monitoring, Analysis, and Reporting Technology (SMART) disk monitoring info with more details.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **show disks** command displays the names of the disks currently attached to the SE.

Table 2-24 describes the fields shown in the **show disks details** display.

Table 2-24 show disks details Field Descriptions

Field	Description
disk00	Availability of the disk: Present, Not present or Not responding, Not used, or (*). **Note** Disk drives that are currently marked as bad are shown as "Not used" in the output. Future bad disk drives (drives that are not used after the next time that the SE is reloaded) are shown with an asterisk (*). Disk identification number and type. Disk size in megabytes and gigabytes.
disk01	Same type of information is shown for each disk.
System use	Amount of disk space being used for system use.
Free	Amount of unused disk space available.

The **show disks error-handling** command displays the current level of disk and sector-related errors.

Table 2-25 describes the fields shown in the **show disks error-handling details** display.

I/O e

Table 2-25 show disks error-handling details Field Descriptions

Field	Description
Disk errors since last boot	Number of disk errors since the device was last rebooted.
Disk total bad sectors	Total number of bad sector errors.
Total errors	Total number of bad sector and disk errors.
Diskname Sector LBA	Each bad sector's Logical Block Address (LBA).
I/O errors	Number of I/O errors.

Proactively Monitoring Disk Health with SMART

The ability to proactively monitor the health of disks with Self Monitoring, Analysis, and Reporting Technology (SMART) was added. SMART provides you with hard drive diagnostic information and information about impending disk failures.

SMART is supported by most disk vendors and is a standard method used to determine the health of a disk. SMART has several read-only attributes (for example, the power-on hours attribute, the load and unload count attribute) that provide the VDS-OS software with information about the operating and environmental conditions that may indicate an impending disk failure.

To display more detailed information, enter the **show disks SMART-info details** command in EXEC configuration mode. The output from the **show disks SMART-info** and the **show disks SMART-info details** commands differ based on the disk vendor and the type of drive technology (Integrated Drive Electronics [IDE], Small Computer Systems Interface [SCSI], and Serial Advanced Technology Attachment [SATA] disk drives).

Even though SMART attributes are vendor dependent, there is a common way of interpreting most SMART attributes. Each SMART attribute has a normalized current value and a threshold value. When the current value exceeds the threshold value, the disk is considered as failed. The VDS-OS software monitors the SMART attributes and reports any impending failure through syslog messages, Simple Network Management Protocol (SNMP) traps, and alarms.

The output from the **show tech-support** command in EXEC configuration mode also includes SMART information.

Table 2-26 describes some typical fields in the **show disks SMART-info** display.

Table 2-26 show disks SMART-info Field Descriptions

Field	Description
disk00—disk05	Shows information for disk drives.
Device Model	Vendor number and version number of the disk.
Serial Number	Serial number for the disk.
Device type	Type of device.
Transport protocol	Physical layer connector information, for example: Parallel SCSI (SPI-4).
Local time is	Day of the week, month, date, time (hh:mm:ss), year, clock standard.
Device supports SMART and SMART is Enabled	Status of SMART support: Enabled or Disabled.

Table 2-26 show disks SMART-info Field Descriptions (continued)

Field	Description
Temperature Warning Enabled	Temperature warning status: Enabled or Disabled.
SMART Health Status:	Health status of the disk: OK or Failed.

Examples

The following example displays output for two disks experiencing sector errors:

```
ServiceEngine# show disks error-handling
Disk errors since last boot:
disk05 total bad sectors = 1, total errors = 2
disk10 total bad sectors = 3, total errors = 9
```

If the **details** option is given, then each bad sector's Logical Block Address (LBA) displays along with its corresponding I/O error count:

```
ServiceEngine# show disks error-handling details
Disk errors since last boot:
 disk05 total bad sectors = 1, total errors = 2
# diskname  Sector (LBA)      I/O errors:
    disk05  3000005           2

disk10 total bad sectors = 3, total errors = 9
# diskname  Sector (LBA)      I/O errors:
    disk10  16000             3
    disk10  170001            4
    disk10  180001            2

Total errors (since system boot) across all disks = 11
```

Note For additional disk health statistics, execute the **show disks smart-info** or **show alarms** commands.

SMART support is vendor dependent; each disk vendor has a different set of supported SMART attributes. The following example shows the output from the **show disks SMART-info** command in EXEC configuration mode that was entered on two different SEs (Service Engine A and Service Engine B). These two SEs contain hard disks that were manufactured by different vendors.

```
ServiceEngine# show disks SMART-info
=== disk00 ===
smartctl version 5.38 [ i686-spcdn-linux-gnu ] Copyright (C) 2002-8 Bruce Allen
Home page is http://smartmontools.sourceforge.net/

=== START OF INFORMATION SECTION ===
Device Model: ST3500320NS
Serial Number: 5QM19RKR
Firmware Version: SN04
User Capacity: 500,107,862,016 bytes
Device is: Not in smartctl database [ for details use: -P showall ]
ATA Version is: 6
ATA Standard is: ATA/ATAPI-6 T13 1410D revision 2
Local Time is: Thu May 21 14:09:19 2009 UTC
SMART support is: Available - device has SMART capability.
SMART support is: Enabled

=== START OF READ SMART DATA SECTION ===
SMART overall-health self-assessment test result: PASSED

RUNNING: /usr/sbin/smartctl /dev/sda -H -i
```

```
=== disk01 ===
smartctl version 5.38 [ i686-spcdn-linux-gnu ] Copyright (C) 2002-8 Bruce Allen
Home page is http://smartmontools.sourceforge.net/

=== START OF INFORMATION SECTION ===
Device Model: ST3500320NS
Serial Number: 5QM19B0B
Firmware Version: SN04
User Capacity: 500,107,862,016 bytes
Device is: Not in smartctl database [ for details use: -P showall ]
ATA Version is: 6
ATA Standard is: ATA/ATAPI-6 T13 1410D revision 2
Local Time is: Thu May 21 14:09:19 2009 UTC
SMART support is: Available - device has SMART capability.
SMART support is: Enabled

=== START OF READ SMART DATA SECTION ===
SMART overall-health self-assessment test result: PASSED

RUNNING: /usr/sbin/smartctl /dev/sdb -H -i

=== disk02 ===
smartctl version 5.38 [ i686-spcdn-linux-gnu ] Copyright (C) 2002-8 Bruce Allen
Home page is http://smartmontools.sourceforge.net/

=== START OF INFORMATION SECTION ===
Device Model: ST3500320NS
Serial Number: 5QM19SK9
Firmware Version: SN04
User Capacity: 500,107,862,016 bytes
Device is: Not in smartctl database [ for details use: -P showall ]
ATA Version is: 6
ATA Standard is: ATA/ATAPI-6 T13 1410D revision 2
Local Time is: Thu May 21 14:09:19 2009 UTC
SMART support is: Available - device has SMART capability.
SMART support is: Enabled

=== START OF READ SMART DATA SECTION ===
SMART overall-health self-assessment test result: PASSED

RUNNING: /usr/sbin/smartctl /dev/sdc -H -i
```

The following example shows the output from the **show dis raid-state** command, which shows all the disk partitions on a CDE:

```
ServiceEngine# #show disks raid-state
SYSTEM : RAID-1
        Status: Normal
        Partitions: disk00/05 disk02/05
SYSTEM: RAID-1
        Status: Normal
        Partitions: disk00/01 disk02/01
SYSTEM: RAID-1
        Status: Normal
        Partitions: disk00/02 disk02/02
SYSTEM: RAID-1
        Status: Normal
        Partitions: disk00/04 disk02/04
```

Related Commands

Command	Description
disk (EXEC)	Configures disks and allocates disk space for devices using VDS-OS software.

show flash

To display the flash memory version and usage information, use the **show flash** command in EXEC configuration mode.

show flash

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

If a new software image has been installed and is waiting to be run after a reboot, the **show flash** command displays this information and the version of VDS-OS software that runs on the device after reload.

Note If you update the VDS-OS software on an SE, the new version displays in the **show flash** command output, but it says, "Pending software change will occur on next bootup." You must reboot the device for the software update to take effect.

Examples

The following example shows how to display the flash information:

```
ServiceEngine# show flash
VDS-OS software version (disk-based code): VDS-OS-2.4.0-b328

System image on flash:
Version: 2.4.0.328

System flash directory:
System image: 274 sectors
Bootloader, rescue image, and other reserved areas: 59 sectors
512 sectors total, 179 sectors free.
```

Table 2-27 describes the fields shown in the **show flash** display.

Table 2-27 show flash Field Descriptions

Field	Description
VDS-OS software version (disk-based code)	VDS-OS software version and build number that is running on the device.
System image on flash:	
Version	Version and build number of the software that is stored in flash memory.
System flash directory:	

Table 2-27 show flash Field Descriptions

Field	Description
System image	Number of sectors used by the system image.
Bootloader, rescue image, and other reserved areas	Number of sectors used by the bootloader, rescue image, and other reserved areas.
XX sectors total, XX sectors free	Total number of sectors. Number of free sectors.

Related Commands

Command	Description
show version	Displays the version information about the software.

show ftp

To display the caching configuration of the File Transfer Protocol (FTP), use the **show ftp** command in EXEC configuration mode.

show ftp

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to display the caching configuration of FTP:

```
ServiceEngine# show ftp

FTP heuristic age-multipliers: directory-listing 30% file 60%
Maximum Time To Live in days : directory-listing 3 file 7
Minimum Time To Live in minutes: 60
No objects are revalidated on every request.
Serve-IMS without revalidation if...
Directory listing object is less than 50% of max age
File object is less than 80% of max age
Incoming Proxy-Mode:
Servicing Proxy mode FTP connections on ports: 22 23 88 66 48 488 449 90
Outgoing Proxy-Mode:
Not using outgoing proxy mode.
Maximum size of a cacheable object is unlimited.
```

Related Commands

Command	Description
ftp	Enables FTP services.

show hardware

To display the system hardware status, use the **show hardware** command in EXEC configuration mode.

show hardware [**all** | **core** | **cpuinfo** | **dmi** [**all** | **baseboard** | **bios** | **cache** | **chassis** | **connector** | **memory** | **processor** | **slot** | **system**] | **mapping** {**disk** [**all** | *diskname*] | **interface** [**all** | **GigabitEthernet** *slot/port_num* | **TenGigabitEthernet** *slot/port_num*]} | **meminfo** | **pci** [**details** | **drivers** | **ids** | **tree**]]

Syntax Description

all	(Optional) Displays all hardware class information.
core	(Optional) Displays core hardware information.
cpuinfo	(Optional) Displays CPU information.
dmi	(Optional) Displays the desktop management interface (DMI).
all	(Optional) Displays all DMI information.
baseboard	(Optional) Displays motherboard information.
bios	(Optional) Displays BIOS information.
cache	(Optional) Displays processor cache information.
chassis	(Optional) Displays chassis information.
connector	(Optional) Displays connector information.
memory	(Optional) Displays physical memory information.
processor	(Optional) Displays processor information.
slot	(Optional) Displays PCI slot information.
system	(Optional) Displays system information.
mapping	(Optional) Shows mapping between Cisco and Linux hardware names.
disk	Maps Cisco disk name to Linux device name.
diskname	Name of the disk (disk00).
interface	Maps Cisco interface name to Linux device name.
all	Displays all interface information.
GigabitEthernet	Selects a 1G ethernet interface.
slot/port_num	Slot and port number for the selected interface. The slot range is from 1 to 14; the port range is from 0 to 0. The slot number and port number are separated with a forward slash character (/).
TenGigabitEthernet	Selects a 10G ethernet interface.
meminfo	(Optional) Displays RAM information.
pci	(Optional) Displays PCI information.
details	(Optional) Show output with PCI addresses and names.
drivers	(Optional) Identify driver names and availability.
ids	(Optional) Show PCI vendor and device codes.
tree	(Optional) Show a tree-like diagram containing all buses, bridges and devices.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The output of the **show hardware** command in EXEC configuration mode displays all core or Desktop Management Interface (DMI) information. The DMI output can also be filtered by optional keywords.

Table 2-28 describes the fields shown in the **show hardware** display.

Table 2-28 show hardware Field Descriptions

Field	Description
Compiled hour:minute:second month day year by cnbuild	Compile information for the software build.
System was restarted on day of week month day hour:minute:second year	Date and time that the system was last restarted.
The system has been up for X hours, X minutes, X seconds	Length of time the system has been running since the last reboot.
CPU 0 is	CPU manufacturer information.
Total X CPU	Number of CPUs on the device.
XXXX Mbytes of Physical memory	Number of megabytes of physical memory on the device.
X CD ROM drive	Number of CD-ROM drives on the device.
X Console interface	Number of console interfaces on the device.
Cookie info	
SerialNumber	Serial number of the device.
SerialNumber (raw)	Serial number of the device as an ASCII value.
TestDate	Date that the device was tested.
ModelNum (text)	Hardware model of the device.
ModelNum (raw)	Internal model number (ASCII value) that corresponds to the ExtModel number.
HWVersion	Number of the current hardware version.
PartNumber	Not implemented.
BoardRevision	Number of revisions for the current system board.
ChipRev	Number of revisions for the current chipset.
VendID	Vendor ID of the cookie.
CookieVer	Version number of the cookie.
Chksum	Checksum of the cookie showing whether the cookie is valid.
List of all disk drives	
Physical disk information	Lists the disks by number.
disk00	Availability of the disk: Present, Not present or Not responding, or Not used (*). Disk identification number and type. Disk size in megabytes and gigabytes.
disk01	Same type of information is shown for each disk.

Table 2-28 show hardware Field Descriptions (continued)

Field	Description
Mounted filesystems	
Device	Path to the partition on the disk.
Type	Type of the file system. Values include PHYS-FS, SYSFS, or CDNFS.
Size	Total size of the file system in megabytes and gigabytes.
Mount point	Mount point for the file system. For example, the mount point for SYSFS is /local/local1.
System use	Amount of disk space being used for system use.
Free	Amount of unused disk space available.
Memory Information	
MemTotal	
MemFree	
Buffers	
Cached	
SwapCached	
Active	
Inactive	
Active(anon)	
Inactive(anon)	
Active(file)	
Inactive(file)	
Unevictable	
Mlocked	
SwapTotal	
SwapFree	
Dirty	
Writeback	
AnonPages	
Mapped	
Shmem	
Slab	
SReclaimable	
SUnreclaim	
KernelStack	
PageTables	
NFS_Unstable	
Bounce	

Table 2-28 show hardware Field Descriptions (continued)

Field	Description
Mounted filesystems	
Device	Path to the partition on the disk.
Type	Type of the file system. Values include PHYS-FS, SYSFS, or CDNFS.
Size	Total size of the file system in megabytes and gigabytes.
Mount point	Mount point for the file system. For example, the mount point for SYSFS is /local/local1.
System use	Amount of disk space being used for system use.
Free	Amount of unused disk space available.
Memory Information	
MemTotal	
MemFree	
Buffers	
Cached	
SwapCached	
Active	
Inactive	
Active(anon)	
Inactive(anon)	
Active(file)	
Inactive(file)	
Unevictable	
Mlocked	
SwapTotal	
SwapFree	
Dirty	
Writeback	
AnonPages	
Mapped	
Shmem	
Slab	
SReclaimable	
SUnreclaim	
KernelStack	
PageTables	
NFS_Unstable	
Bounce	

Table 2-28 show hardware Field Descriptions (continued)

Field	Description
WritebackTmp	
CommitLimit	
Committed_AS	
VmallocTotal	
VmallocUsed	
VmallocChunk	
DirectMap4k	
DirectMap2M	
PCI Information	

Examples

The following example shows how to display the core hardware information:

```
ServiceEngine# show hardware core
Videoscape Distribution Suite Origin Server Software (VDS-OS)
Copyright (c) 1999-2011 by Cisco Systems, Inc.
Videoscape Distribution Suite Origin Server Software Release 2.6.0 (build
b460 Aug 28 2011)
Version: cde220-2g2-DEVELOPMENT[vcn-build1:/auto/v
cn-u1/vosis_release_builds/vosis_2.6.0-b460/spcdn]

Compiled 05:55:01 Aug 28 2011 by ipvbuild
Compile Time Options: KQ SS

System was restarted on Mon Aug 29 11:56:58 2011.
The system has been up for 1 day, 5 hours, 5 minut
es, 2 seconds.

CPU 0 is GenuineIntel Intel(R) Xeon(R) CPU
   L5410 @ 2.33GHz (rev 23) running at 2333MHz.
CPU 1 is GenuineIntel Intel(R) Xeon(R) CPU
   L5410 @ 2.33GHz (rev 23) running at 2333MHz.
CPU 2 is GenuineIntel Intel(R) Xeon(R) CPU
   L5410 @ 2.33GHz (rev 23) running at 2333MHz.
CPU 3 is GenuineIntel Intel(R) Xeon(R) CPU
   L5410 @ 2.33GHz (rev 23) running at 2333MHz.
CPU 4 is GenuineIntel Intel(R) Xeon(R) CPU
   L5410 @ 2.33GHz (rev 23) running at 2333MHz.
CPU 5 is GenuineIntel Intel(R) Xeon(R) CPU
   L5410 @ 2.33GHz (rev 23) running at 2333MHz.
CPU 6 is GenuineIntel Intel(R) Xeon(R) CPU
   L5410 @ 2.33GHz (rev 23) running at 2333MHz.
CPU 7 is GenuineIntel Intel(R) Xeon(R) CPU
   L5410 @ 2.33GHz (rev 23) running at 2333MHz.
Total 8 CPUs.
16000 Mbytes of Physical memory.
10 GigabitEthernet interfaces
1 Console interface
2 USB interfaces [Not supported in this version of
 software]

  Cookie info:
```

```
    Base PID: CDE220-2G2                VID: 00
    SerialNumber: 99999999999
    Model Type:
    SerialNumber (raw): 57 57 57 57 57 57 57 57 57
 57 57
    TestDate: 12-19-2002
    ExtModel: CDE220-2G2
    ModelNum (raw): 55 0 0 0 1
    HWVersion: 1
    PartNumber: 53 54 55 56 57
    BoardRevision: 1
    ChipRev: 1
    VendID: 0
    CookieVer: 2
    Chksum: 0xfb9e

List of all disk drives:
disk00: Normal          (h02 c00 i00 l00 -       m
ptsas)  476940MB(465.8GB)
        disk00/01: SYSTEM         5120MB[  5.0GB)
mounted internally
        disk00/02: SYSTEM         3072MB[  3.0GB)
mounted internally
        disk00/04: SYSTEM         2048MB[  2.0GB)
mounted internally
        disk00/05: SYSFS         32768MB[ 32.0GB)
mounted at /local1
        disk00/06: CDNFS        433917MB(423.7GB)
mounted internally
disk01: Normal          (h02 c00 i01 l00 -       m
ptsas)  476940MB(465.8GB)
        disk01/01: SYSTEM         5120MB[  5.0GB)
mounted internally
        disk01/02: SYSTEM         3072MB[  3.0GB)
mounted internally
        disk01/04: SYSTEM         2048MB[  2.0GB)
mounted internally
        disk01/05: SYSFS         32768MB[ 32.0GB)
mounted at /local1
<Output truncated>
```

The following example shows how to display the DMI information:

```
ServiceEngine# show hardware dmi
---------------------- DMI Information -------------
# dmidecode 2.9
SMBIOS 2.5 present.
70 structures occupying 2793 bytes.
Table at 0xCFF66000.

Handle 0x0000, DMI type 0, 24 bytes
BIOS Information
        Vendor: Phoenix Technologies LTD
        Version: 1.2a
        Release Date: 04/09/2009
        Address: 0xE3DD0
        Runtime Size: 115248 bytes
        ROM Size: 2048 kB
        Characteristics:
                PCI is supported
                PNP is supported
                BIOS is upgradeable
                BIOS shadowing is allowed
                ESCD support is available
```

```
                Boot from CD is supported
ServiceEngine#
```

Related Commands

Command	Description
show version	Displays version information about the SE software.

show hosts

To view the hosts on your SE, use the **show hosts** command in EXEC configuration mode.

show hosts

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Examples

The **show hosts** command lists the name servers and their corresponding IP addresses. It also lists the hostnames, their corresponding IP addresses, and their corresponding aliases (if applicable) in a host table summary.

Table 2-29 describes the fields shown in the **show hosts** display.

Table 2-29 show hosts Field Descriptions

Field	Description
Domain names	Domain names used by the device to resolve the IP address.
Name Server(s)	IP address of the Domain Name System (DNS) name server or servers.
Host Table	
hostname	Fully qualified domain name (FQDN) (that is, hostname and domain) of the current device.
inet address	IP address of the current host device.
aliases	Name configured for the current device based on the **host** command in global configuration mode.

show interface

To display the hardware interface information, use the **show interface** command in EXEC configuration mode.

show interface {**all** | **GigabitEthernet** *slot/port* | **PortChannel** {**1** [**lacp**] | **2**} | **standby** *group_num* | **TenGigabitEthernet** *slot/port*}

Syntax Description

all	Displays information for all interfaces.
GigabitEthernet	Displays information for the Gigabit Ethernet device.
slot/port	Slot and port number for the selected interface. The range is from 1 to 14. The slot number and port number are separated with a forward slash character (/).
PortChannel	Displays information for the Ethernet channel of the device.
1	Sets the Ethernet channel interface number to 1.
lacp	(Optional) Displays the LACP port channel status.
2	Sets the Ethernet channel interface number to 2.
standby	Displays information for the standby group for the interface.
group_num	Group number for the selected interface. The group number range is 1 to 4.
TenGigabitEthernet	Displays information for the Ten Gigabit Ethernet device.
slot/port	Slot and port number for the selected interface. The range is from 1 to 14. The slot number and port number are separated with a forward slash character (/).

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-30 describes the fields shown in the **show interface GigabitEthernet** display.

Table 2-30 show interface GigabitEthernet Field Descriptions

Field	Description
Type	Type of interface. Always Ethernet.
Ethernet address	Layer 2 Media Access Control (MAC) address.
Maximum Transfer Unit Size	Current configured maximum transmission unit (MTU) value.
Metric	Metric setting for the interface. The default is 1. The routing metric is used by the routing protocol to determine the most favorable route. Metrics are counted as additional hops to the destination network or host; the higher the metric value, the less favorable the route.
Packets Received	Total number of packets received by this interface.

Table 2-30 show interface GigabitEthernet Field Descriptions (continued)

Field	Description
Input Errors	Number of incoming errors on this interface.
Input Packets Dropped	Number of incoming packets that were dropped on this interface.
Input Packets Overruns	Number of incoming packet overrun errors.
Input Packets Frames	Number of incoming packet frame errors.
Packet Sent	Total number of packets sent from this interface.
Output Errors	Number of outgoing packet errors.
Output Packets Dropped	Number of outgoing packets that were dropped by this interface.
Output Packets Overruns	Number of outgoing packet overrun errors.
Output Packets Carrier	Number of outgoing packet carrier errors.
Output Queue Length	Output queue length in bytes.
Collisions	Number of packet collisions at this interface.
Flags	Interface status indicators. Values include Up, Broadcast, Running, and Multicast.
Mode	Setting, transmission mode, and transmission for this interface.

Table 2-31 describes the fields shown in the **show interface PortChannel** display.

Table 2-31 show interface PortChannel Field Descriptions

Field	Description
Description	Description of the device, as configured by using the **description** keyword of the **interface** command in global configuration mode.
Type	Type of interface. Always Ethernet.
Ethernet address	Layer 2 MAC address.
Internet Address	Internet IP address configured for this interface.
Broadcast Address	Broadcast address configured for this interface.
Netmask	Netmask configured for this interface.
IPv6	IPv6 address of the interface.
Maximum Transfer Unit Size	Current configured MTU value.
Metric	Metric setting for the interface. The default is 1. The routing metric is used by the routing protocol. Higher metrics have the effect of making a route less favorable; metrics are counted as addition hops to the destination network or host.
Packets Received	Total number of packets received by this interface.
Input Errors	Number of incoming errors on this interface.
Input Packets Dropped	Number of incoming packets that were dropped on this interface.

Table 2-31 show interface PortChannel Field Descriptions (continued)

Field	Description
Input Packets Overruns	Number of incoming packet overrun errors.
Input Packets Frames	Number of incoming packet frame errors.
Packet Sent	Total number of packets sent from this interface.
Output Errors	Number of outgoing packet errors.
Output Packets Dropped	Number of outgoing packets that were dropped by this interface.
Output Packets Overruns	Number of outgoing packet overrun errors.
Output Packets Carrier	Number of outgoing packet carrier errors.
Output Queue Length	Output queue length in bytes.
Collisions	Number of packet collisions at this interface.
Flags	Interface status indicators. Values include Up, Broadcast, Running, and Multicast.
Interface PortChannel 1 (8 physical interface(s)	
Protocol	Indicates if the LACP is turned on or off.
Mode	Port channel load balancing method (dst-ip, dst-mix-ip-port, dst-port, round-robin, src-dst-ip, src-dst-mac, src-dst-mixed-ip-port, src-dst-port, src-mixed-ip-port, src-port)
Port ID	Interface name.
Admin-State	Interface admin state. This is the interface state that the user configured from the command line. For example, if the user configured “no shut” on the interface, the admin state is up.
Link-State	Interface physical status. Indicates if the link is up or down.
LACP-State	Provides a better detection for the link status through LACP protocol. It tells the upper layer if the physical link is up or down.
Aggregate ID	When LACP is turned on, the interface on the same port channel is grouped into the same aggregate ID.

Table 2-32 describes the fields shown in the **show interface standby** display.

Table 2-32 show interface standby Field Descriptions

Field	Description
Standby Group	Number that identifies the standby group.
Description	Description of the device, as configured by using the **description** keyword of the **interface** command in global configuration mode.
IP address, netmask	IP address and netmask of the standby group.

Table 2-32 show interface standby Field Descriptions (continued)

Field	Description
Member interfaces	Member interfaces of the standby group. Shows which physical interfaces are part of the standby group. Shows the interface definition, such as GigabitEthernet 1/0.
Active interface	Interfaces that are currently active in the standby group.

Table 2-33 describes the fields shown in the **show interface TenGigabitEthernet** display.

Table 2-33 show interface TenGigabitEthernet Field Descriptions

Field	Description
Type	Type of interface. Always Ethernet.
Ethernet address	Layer 2 MAC address.
Internet address	Internet IP address configured for this interface.
Broadcast address	Broadcast address configured for this interface.
Netmask	Netmask configured for this interface.
IPv6 address	IPv6 address of the interface.
Maximum Transfer Unit Size	Current configured MTU value.
Metric	Metric setting for the interface. The default is 1. The routing metric is used by the routing protocol to determine the most favorable route. Metrics are counted as additional hops to the destination network or host; the higher the metric value, the less favorable the route.
Packets Received	Total number of packets received by this interface.
Input Errors	Number of incoming errors on this interface.
Input Packets Dropped	Number of incoming packets that were dropped on this interface.
Input Packets Overruns	Number of incoming packet overrun errors.
Input Packets Frames	Number of incoming packet frame errors.
Packet Sent	Total number of packets sent from this interface.
Output Errors	Number of outgoing packet errors.
Output Packets Dropped	Number of outgoing packets that were dropped by this interface.
Output Packets Overruns	Number of outgoing packet overrun errors.
Output Packets Carrier	Number of outgoing packet carrier errors.
Output Queue Length	Output queue length in bytes.
Collisions	Number of packet collisions at this interface.
Interrupts	Number of interrupts on this interface.
Flags	Interface status indicators. Values include Up, Broadcast, Running, and Multicast.

Related Commands

Command	Description
interface	Configures a Gigabit Ethernet or port channel interface.
lacp	Turns on LACP.
show lacp	Displays LACP information.
show running-config	Displays the current running configuration information on the terminal.
show startup-config	Displays the startup configuration.

show inventory

To display the system inventory information, use the **show inventory** command in EXEC configuration mode.

show inventory

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **show inventory** command allows you to view the unique device identifier information (UDI) for an SE. Typically, Cisco SEs contain the following three identification items that make up the UDI:

- Product ID (PID)
- Version ID (VID)
- Serial number (SN)

This identity information is stored in the SE nonvolatile memory. Each SE has a UDI. The UDI shows PID, VID and SN.

The UDI is electronically accessed by the product operating system or network management application to enable identification of unique hardware devices. The data integrity of the UDI is vital to customers. The UDI that is programmed into the SE's nonvolatile memory is equivalent to the UDI that is printed on the product label and on the carton label. This UDI is also equivalent to the UDI that can be viewed through any electronic means and in all customer-facing systems and tools. Currently, there is only CLI access to the UDI; there is no Simple Network Management Protocol (SNMP) access to the UDI information.

On newer SE models, you can use the **show inventory** command in EXEC configuration mode to display the SE's UDI. On older SE models, use the **show tech-support** command in EXEC configuration mode to display the SE's UDI.

Examples

The following example shows the inventory information for one of the newer SE models (SE-565):

```
ServiceEngine# show inventory

PID: SE-565-K9 VID: 0 SN: serial_number
```

In the preceding example, *serial number* is the serial number of the SE. The version ID is displayed as "0" because the version number is not available.

Table 2-34 describes the fields shown in the **show inventory** display.

Table 2-34 show inventory Field Descriptions

Field	Description
PID	Product ID number of the device.
VID	Version ID number of the device. Displays as 0 if the version number is not available.
SN	Serial number of the device.

The following example shows that you must use the **show tech-support** command in EXEC configuration mode to display the inventory information on an older SE model:

```
ServiceEngine# show inventory
Please look at 'sh tech-support' for information!
ServiceEngine# show tech-support
```

Related Commands

Command	Description
show tech-support	Displays system information necessary for Cisco Technical Support to assist you with your SE.

show ip

To display the, use the **show ip** command in user EXEC configuration mode.

show ip

Syntax Description

ip_address	(Optional) IP address entered to filter the output to display only a particular host in the Border Gateway Protocol (BGP) routing table.
prefix	(Optional) Prefix entered to filter the output to display only a particular network in the BGP routing table.
prefix_length	(Optional) Specifies the prefix length.

Command Default

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

To display information about an entry in the BGP routing table (for example, 42.1.1.0/24), use the **show ip bgp 42.1.1.0/24** command. To locate information by IP address (for example, 42.1.1.1), use the **show ip bgp 42.1.1.1** command.

```
ServiceRouter# show ip bgp 42.1.1.0/24
BGP routing table entry for 42.1.1.0/24, version 12
Paths: (1 available, best # 1)
Flags: on xmit-list, is in urib, is best urib route

  Path type: internal, path is valid, is best path
  AS-Path: NONE, path sourced internal to AS
    192.168.86.3 (metric 0) from 192.168.86.3 (192.168.86.3)
      Origin incomplete, MED 0, localpref 100, weight 0

  Not advertised to any peer

ServiceRouter# show ip bgp 42.1.1.1

BGP routing table entry for 42.1.1.0/24, version 12
Paths: (1 available, best # 1)
Flags: on xmit-list, is in urib, is best urib route

  Path type: internal, path is valid, is best path
  AS-Path: NONE, path sourced internal to AS
    192.168.86.3 (metric 0) from 192.168.86.3 (192.168.86.3)
      Origin incomplete, MED 0, localpref 100, weight 0

Not advertised to any peer

ServiceRouter#
```

The following sample output shows the display when the advertised community and the configured location community matches:

```
ServiceRouter# sh ip bgp 1.1.1.1
BGP routing table entry for 1.1.1.1/32, version 4
Paths: (1 available, best # 1)
Flags: on xmit-list, is in urib, is best urib route

Path type: internal, path is valid, is best path
  AS-Path: NONE, path sourced internal to AS
    48.0.0.8 (metric 0) from 48.0.0.8 (1.1.1.1)
      Origin IGP, MED 0, localpref 100, weight 0
      Community: 1:1(location specific)
```

The following sample output shows the display when the community is not advertised to any peer:

```
ServiceRouter# sh ip bgp 33.1.5.0

BGP routing table entry for 33.1.5.0/24, version 4
Paths: (1 available, best #1)
Flags: on xmit-list, is in urib, is best urib route

  Path type: internal, path is valid, is best path
  AS-Path: 2 , path sourced external to AS
    62.0.0.2 (metric 20) from 26.0.0.6 (10.1.1.1)
      Origin IGP, MED 0, localpref 100, weight 0
      Community: 5:5(location specific)
```

Related Commands

Command	Description
clear ip bgp	Clears entries in the BGP route table.
router bgp	Configures a BGP routing process.

show ipv6

To display IPv6 information, use the **show ipv6** command in user EXEC configuration mode.

show ipv6

Syntax Description

access-list	Displays IPv6 access list information.
standard_ip_acl_num	Standard IPv6 access-list number. The range is from 1 to 99.
extended_ip_acl_num	Extended IPv6 access-list number. The range is from 100 to 199.
access-list name	Access-list name (max 30 characters).
routes	Displays the IPv6 routing table.

Command Default

None

Command Modes

User EXEC configuration mode.

Examples

The following example shows sample output from the **show ipv6 access-list** command:

```
ServiceRouter# show ipv6 access-list
Space available:
    48 access lists
   498 access list conditions

Standard IPv6 access list 1
   1 deny fec0:0:3:5: :1/128
     (implicit deny any: 0 matches)
   total invocations: 0
Extended IPv6 access list test
   1 permit icmpv6 any any echo
     (implicit fragment permit: 0 matches)
     (implicit deny ip any any: 0 matches)
   total invocations: 0

Interface access list references:
  None Configured

Application access list references:
  No applications registered.
```

The following example shows sample output from the **show ipv6 routes** command:

```
ServiceRouter# show ipv6 routes
Destination                              Next Hop
---------------------------------------- ----------------------------------
Destination                              Next
3ffe:1200:4260:f: :/64                   : :
fe80: :/64                               : :
fec0:0:3:3: :/64                         : :
ff00: :/8                                : :
: :/0                                    fec0:0:3:3: :1
: :/0                                    fe80: :218:74ff:fe17:a8c0
ServiceRouter#
```

Note On other **show** commands that relate to the IPv6 addresses, the output fields were designed to work with the longest possible IPv4 address, which has 15 characters; IPv6 addresses can be up to 39 characters long. When the command output displays an IPv6 address, a long IPv6 address can overflow into neighboring fields causing the output to be difficult to read.

Related Commandsl

Command	Description
clear ipv6	Clears IPv6 ACL counters.
ipv6	Specifies the default gateway's IPv6 address.
traceroute6	Traces the route to a remote IPv6-enabled host.

show lacp

To display LACP information, use the **show lacp** command in EXEC configuration mode.

show lacp {**counters**| **internal**}

Syntax Description		
	counters	Displays LACP traffic information.
	internal	Displays LACP link status information.

Defaults None

Command Modes EXEC configuration mode.

Usage Guidelines You must first turn on LACP by entering the **lacp** command in interface configuration mode before you can display the LACP statistics.

In the **show lacp counters** command, the LACP control packet is sent or received every 30 seconds. If one of the interfaces within the port channel goes down, then the counter value does not further increment for that interface.

Examples The following example shows how to display the LACP statistics:

```
ServiceEngine# show lacp counters
Interface PortChannel 1 (4 physical interface(s)):
Protocol: none

Interface PortChannel 2 (4 physical interface(s)):
                          lacpdu             marker     marker response
Port                  send       receive    send  receive send receive error
-----------------------------------------------------
GigabitEthernet  7/0         16         16      0      0      0      0      0
GigabitEthernet  8/0         16         15      0      0      0      0      0
GigabitEthernet  9/0         16         15      0      0      0      0      0
GigabitEthernet 10/0         17         15      0      0      0      0      0

Interface PortChannel 3 (0 physical interface(s)):
Protocol: none

Interface PortChannel 4 (0 physical interface(s)):
Protocol: none
```

The following example shows how to display the link status for the port channel:

```
ServiceEngine# show lacp internal
Interface PortChannel 1 (4 physical interface(s)):
Protocol: LACP
Mode:     src-dst-port
Port                    Admin-State Link-State     LACP-State     Aggregate id
-------------------------------------------------------------------------------
GigabitEthernet  3/0           up         up         bndl              21
GigabitEthernet  4/0           up         up         bndl              21
```

```
GigabitEthernet  5/0           up         up         bndl              21
GigabitEthernet  6/0           up         up         bndl              21

ServiceEngine# show interface portChannel 1 lacp
Interface PortChannel 1 (4 physical interface(s)):
Protocol: LACP
Mode:     src-dst-port
Port                    Admin-State Link-State     LACP-State     Aggregate id
------------------------------------------------------------------------------
GigabitEthernet  3/0           up         up         bndl              21
GigabitEthernet  4/0           up         up         bndl              21
GigabitEthernet  5/0           up         up         bndl              21
GigabitEthernet  6/0           up         up         bndl              21
```

Related Commands

Command	Description
lacp	Turns on Link Aggregation Control Protocol (LACP).
show interface portchannel 1 lacp	Displays the link status for the port channel.

show logging

To display the system message log configuration, use the **show logging** command in EXEC configuration mode.

show logging

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The following is an example of a syslog message for proxy mode native File Transfer Protocol (FTP) support:

```
SE-FTP_PROXY-3-252009:   Failed to configure FTP Proxy-mode listener on port
                    ' [ port ] '.

Explanation:        Could not start proxy-mode listener for FTP control
                    connection for the specified port. The port is temporarily
                    in an un-bindable state, or is in use by some other
                    application.

Action:             Check whether the port has been configured for use by a
                    different application. If not, retry the
                    incoming proxy command after 2 minutes. If this error
                    repeats frequently, contact Cisco TAC.
```

To view information about events that have occurred in all devices in your VDS-OS network, you can use the system message log in the VOSM GUI. The VOSM logs only severity level critical or higher messages from registered nodes. Also, the VOSM logs certain other status messages that are considered important to the Centralized Management System (CMS). The messages displayed in the system message log for device, SE, are not related to the messages logged in the system log file on the system file system (sysfs) partition on the VOSM as /local1/syslog.txt.

The syslog.txt file on the VOSM contains information about events that have occurred on the VOSM and not on the registered nodes. The messages that are written to the syslog.txt file depend on specific parameters of the system log file that you have set by using the **logging** global configuration command. For example, a critical error message logged on a registered node does not appear in the syslog.txt file on the VOSM because the problem never occurred on the VOSM but only on the registered node. However, this error message is displayed in the system message log for device the SE device.

Examples

The following example shows how to display the syslog host configuration on an SE:

```
ServiceEngine# show logging
Syslog to host is disabled
Priority for host logging is set to: warning

Syslog to console is disabled
Priority for console logging is set to: warning

Syslog to disk is enabled
Priority for disk logging is set to: notice
Filename for disk logging is set to: /local1/syslog.txt

Syslog facility is set to *

Syslog disk file recycle size is set to 500000
```

Related Commands

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.
logging	Configures system logging.

show mount-option

To display the mount options, use the **show mount-option** command in EXEC configuration mode.

show mount-option

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-35 describes the fields shown in the **show mount-option** display.

Table 2-35 show mount-option status Field Descriptions

Field	Description
Read/Write	
ReadBlock Size	
WriteBlock Size	
Mount Timeout	
Retransmit	
Retry Minutes	

Related Commands

Command	Description
mount-option	Configures the mount option profile for remote storage.

show ntp

To display the Network Time Protocol (NTP) parameters, use the **show ntp** command in EXEC configuration mode.

show ntp status

Syntax Description

status	Displays the NTP status.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-35 describes the fields shown in the **show ntp status** display.

Table 2-36 show ntp status Field Descriptions

Field	Description
NTP	Status of whether NTP is enabled or disabled.
server list	NTP server IP and subnet addresses.
remote	Name (first 15 characters) of remote NTP server.
*	In the remote column, identifies the system peer to which the clock is synchronized.
+	In the remote column, identifies a valid or eligible peer for NTP synchronization.
space	In the remote column, indicates that the peer was rejected. (The peer could not be reached or excessive delay occurred in reaching the NTP server.)
x	In the remote column, indicates a false tick and is ignored by the NTP server.
-	In the remote column, indicates a reading outside the clock tolerance limits and is ignored by the NTP server.
refid	Clock reference ID to which the remote NTP server is synchronized.
st	Clock server stratum or layer.
t	Type of peer (local, unicast, multicast, or broadcast).
when	Status of when the last packet was received from the server, in seconds.
poll	Time check or correlation polling interval, in seconds.
reach	8-bit reachability register. If the server was reachable during the last polling interval, a 1 is recorded; otherwise, a 0 is recorded. Octal values 377 and above indicate that every polling attempt reached the server.
delay	Estimated delay (in milliseconds) between the requester and the server.
offset	Clock offset relative to the server.
jitter	Clock jitter.

Related Commands

Command	Description
clock	Sets or clears clock functions or updates the calendar.
ntp	Configures the Network Time Protocol (NTP) server and allows the system clock to be synchronized by a time server.

show processes

To display CPU or memory processes, use the **show processes** command in EXEC configuration mode.

show processes [**cpu** | **debug** *pid* | **memory** | **system** [**delay** *delay_num* | **count** *count_num*]]

Syntax Description

cpu	(Optional) Displays the CPU utilization.
debug	(Optional) Displays the system call and signal traces for a specified process identifier (PID) to display system progress.
pid	Process identifier.
memory	(Optional) Displays memory allocation processes.
system	(Optional) Displays system load information in terms of updates.
delay	(Optional) Specifies the delay between updates, in seconds. The range is from 1 to 60.
delay_num	Displays delays between updates, in seconds.
count	(Optional) Specifies the number of updates that are displayed. The range is from 1 to 100.
count_num	Displays the number of updates displayed.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use the commands shown in this section to track and analyze system CPU utilization.

The **show processes debug** command displays the extensive internal system call information and a detailed account of each system call (and arguments) made by each process and the signals that it has received.

Use the **show processes system** command to display system updates. The **delay** option specifies the delay between updates, in seconds. The **count** option specifies the number of updates that are displayed. This command displays these items:

- List of all processes in wide format.
- Two tables listing the processes that use CPU resources. The first table displays the list of processes in descending order of utilization of CPU resources based on a snapshot taken after the processes system (ps) output is displayed. The second table displays the same processes based on a snapshot taken 5 seconds after the first snapshot.
- Virtual memory used by the corresponding processes in a series of five snapshots, each separated by 1 second.

Note CPU utilization and system performance may be affected when you use the **show process** command. We recommend that you avoid using the s**how process** command with keywords **system** and especially **debug,** unless it is absolutely necessary.

Table 2-37 describes the fields shown in the **show processes** displays.

Table 2-37 show processes Field Descriptions

Field	Description
CPU Usage	CPU utilization as a percentage for user, system overhead, and idle.
PID	Process identifier.
STATE	Current state of corresponding processes: R = Running S = Sleeping in an interruptible wait D = Sleeping in an uninterruptible wait or swapping Z = Zombie T = Traced or stopped on a signal
PRI	Priority of processes.
User T	User time utilization, in seconds.
Sys T	System time utilization, in seconds.
COMMAND	Process command.
Total	Total available memory, in bytes.
Used	Memory currently used, in bytes.
Free	Free memory available, in bytes.
Shared	Shared memory currently used, in bytes.
Buffers	Buffer memory currently used, in bytes.
Cached	Cache memory currently used, in bytes.
TTY	TTY to which the process is attached. For example, TTY may indicate which processes belong to network Telnet sessions.
%MEM	Percentage of memory used by corresponding processes.
VM Size	Virtual memory size (in bytes) allocated to the corresponding process.
RSS (pages)	Resident set size, which indicates the number of pages that the process has in real memory minus three (–3) for administrative purposes. These pages count toward text, data, and stack space, but do not count demand-loaded or swapped-out pages.
Name	Filename of the executable, in parentheses.

show radius-server

To display RADIUS information, use the **show radius-server** command in EXEC configuration mode.

show radius-server

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-38 describes the fields shown in the **show radius-server** display.

Table 2-38 show radius-server Field Descriptions

Field	Description
Login Authentication for Console/Telnet Session	Status of whether RADIUS server is enabled for login authentication.
Configuration Authentication for Console/Telnet Session	Status of whether RADIUS server is enabled for authorization or configuration authentication.
Authentication scheme fail-over reason	Status of whether SEs fail over to the secondary method of administrative login authentication whenever the primary administrative login authentication method fails.
RADIUS Configuration	RADIUS authentication settings.
RADIUS Authentication	Status of whether RADIUS authentication is enabled on the SE.
Key	Key used to encrypt and authenticate all communication between the RADIUS client (the SE) and the RADIUS server.
Timeout	Number of seconds that the SE waits for a response from the specified RADIUS Authentication Server before declaring a timeout.
Retransmit	Number of times that the SE is to retransmit its connection to the RADIUS if the RADIUS timeout interval is exceeded.
Radius Redirect	Status of whether the RADIUS server redirects the response if an authentication request fails.
Reply-Message	Message sent to the user if redirection occurs.
URL(s) to authentication failure instructions expired	HTML page location or URL where the redirect message should be sent.
Servers	RADIUS servers that the SE is to use for RADIUS authentication.

Table 2-38 show radius-server Field Descriptions (continued)

Field	Description
IP	Hostname or IP address of the RADIUS server.
Port	Port number on which the RADIUS server is listening.

Related Commands

Command	Description
radius-server	Configures RADIUS authentication parameters.

show running-config

To display the current running configuration information on the terminal, use the **show running-config** command in EXEC configuration mode.

show running-config

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use this command with the **show startup-config** command to compare the information in running memory to the startup configuration used during bootup.

Note This command replaces the **write terminal** command.

Examples

The following example shows how to display the current running configuration information:

```
ServiceEngine# show running-config
! VDS-OS version 2.6.0
!
device mode service-engine
!
hostname EE8-2G2-5
!
authsvr location-server primary 4.0.1.3 7000
!
clock timezone PDT -7 0
!
ip domain-name telstra.com
!
exec-timeout 0
!
interface PortChannel 1
 ip address 188.0.82.8 255.255.255.0
 exit
interface PortChannel 2
 ip address 188.87.0.5 255.255.0.0
 exit
!
interface GigabitEthernet 1/0
 channel-group 1
 exit
interface GigabitEthernet 2/0
 channel-group 1
 exit
interface GigabitEthernet 3/0
```

```
 channel-group 2
 exit
interface GigabitEthernet 4/0
 channel-group 2
 exit
interface GigabitEthernet 5/0
 channel-group 2
 exit
interface GigabitEthernet 6/0
 channel-group 2
 exit
interface GigabitEthernet 7/0
 channel-group 2
 exit
interface GigabitEthernet 8/0
 channel-group 2
 exit
interface GigabitEthernet 9/0
 channel-group 2
 exit
interface GigabitEthernet 10/0
 channel-group 2
 exit
!
streaming-interface PortChannel 2
!
ip default-gateway 188.0.82.1
ip default-gateway 188.87.0.1
!
port-channel load-balance round-robin
primary-interface PortChannel 2
!
transaction-logs enable
transaction-logs archive max-file-size 2000000
transaction-logs archive max-file-number 50
transaction-logs archive interval 300
transaction-logs export enable
transaction-logs export interval 5
transaction-logs export sftp-server 188.0.84.5 root **** /var/ftp/pub/
upload
transaction-logs format custom "%J"
!
ip name-server 188.0.84.7
!
ip route 10.74.61.0 255.255.255.0 188.87.0.1
ip route 171.70.77.0 255.255.255.0 188.87.0.1
ip route 188.85.0.3 255.255.255.255 188.87.0.1
ip route 188.0.86.3 255.255.255.255 188.0.82.1
ip route 188.85.0.4 255.255.255.255 188.87.0.1
ip route 225.1.1.12 255.255.255.255 188.87.0.1
ip route 239.1.1.12 255.255.255.255 188.87.0.1
ip route 239.1.1.14 255.255.255.255 188.87.0.1
ip route 224.0.0.22 255.255.255.255 188.87.0.1
!
ntp server 171.68.10.150
ntp server 171.68.10.80
!
rule enable
!
username admin password 1 $5$bVz2jc/k$QYvCAKrBmq3YqM5IklvuGrXQACMelfON
dq3/siTpqV8
username admin privilege 15
!
snmp-server enable traps config
```

```
snmp-server enable traps service-engine disk-fail
snmp-server enable traps alarm raise-critical
snmp-server enable traps alarm clear-critical
snmp-server enable traps alarm raise-major
snmp-server enable traps alarm clear-major
snmp-server enable traps alarm raise-minor
snmp-server enable traps alarm clear-minor
snmp-server enable traps entity
snmp-server enable traps snmp cold-start
snmp-server host 188.0.84.6 telstra v2c
snmp-server group telstra v2c read telstra notify telstra
snmp-server community telstra
!
tacacs key ****
tacacs password ascii
tacacs host 188.0.84.5 primary
!
ftp enable
!
telnet enable
!
VOSM ip 188.0.86.3
cms enable
!
cms database maintenance regular schedule every-day at 04:00
cms database maintenance full schedule Sun at 04:00
!
kernel kdb
disk error-handling reload
!
banner enable
!
url-signature key-id-owner 1 key-id-number 1 key ****
url-signature key-id-owner 2 key-id-number 2 key ****
!
contentmgr disk-bucket-fail-threshold 1
!
! End of VDS-OS configuration
ServiceEngine#
```

Related Commands

Command	Description
configure	Enters global configuration mode.
copy	Copies the configuration or image data from a source to a destination.

show service-router

To display the Service Router configuration, use the **show service-router** command in EXEC configuration mode.

On the SE:

show service-router {**keepalive-interval** | **service-monitor**}

On the SR:

show service-router {**forwarding** [**content-origin** *content_origin*] | **lastresort** [**domain** *name*] | **load** {**all** | **sename** *sename*} | **memory** | **redirect-burst-control** | **routes** [**content-origin** *content_origin* **ip-address** *ip_address*] | **service-monitor** | **services** {**all** | **sename** *se_name*} | **summary** [**content-origin** *content_origin*]}

On the VOSM:

show service-router service-monitor

Syntax Description

forwarding	Displays the content origin forwarding tables.
content-origin	(Optional) Displays information for one content origin.
content_origin	Content origin fully qualified domain name (FQDN).
lastresort	Displays the domain and alternate domain configured.
domain	(Optional) Displays information for one domain.
name	Domain name.
load	Displays the load and threshold reached status.
all	Displays for all SEs.
sename	Displays for one SE.
se_name	SE name.
memory	Displays details on malloc-related memory usage for the SR process.
proximity-based-routing	Displays the proximity-based routing configurations.
cache	(Optional) Displays proximity-based routing cache information.
ip	Displays one IP address or subnet.
ip_address	Client IP address or subnet of the proximity cache information to be displayed.
redirect-burst-control	Displays the redirect burst control configurations.
routes	Displays the content origin routing tables.
service-monitor	Displays the service monitor configuration.
services	Displays the services status.
summary	Displays the content origin routing table summary statistics.
keepalive-interval	Displays the keepalive interval.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

This command allows users to check the Service Router-related configuration. Through this command, users can view the configured features of an SR, such as location-based routing and content-based routing.

Note The Load percentage displayed in the Average Device Load field when the **show service-router service-monitor** command is executed on the SE is the maximum of the average disk load/average CPU load given both CPU and disk monitoring are enabled on the SE.

The memory usage is calculated in the **show service-router service-monitor** command as follows:

Total used memory = total memory - (total free memory + total buffer memory + total cache memory) + total pinned memory. The percentage of total used memory = (total used memory)/total memory.

The total memory, total free memory, total buffer memory, and total cache memory are obtained from /proc/meminfo. The total pinned memory is obtained from /proc/ukse/ukse_prefetch_details.

The **show service-router content-origin <content-origin> ip-address <client-ip>** command is only used to check which SE the request is routed to based on the network entries and metrics configured in the coverage zone file. It does not take into account the service status of the SEs because there is no protocol or filename in the input. Also, it does not take into account matches from location based routing and proximity based routing.

The **show service-router content-origin <content-origin>** output shows an SE as overloaded only if the device load has exceeded thresholds. The SE does not show as overloaded because there might be other Protocol Engines in the SE that are still able to serve requests.

Examples

The following example shows how to display SR routing statistics:

```
ServiceRouter# show statistics service-router all | begin "SR Routing Statistics"
----- SR Routing Statistics -----
    Network Redirects         :                 0
    Proximity Redirects       :                 2
    Geo Location Redirects    :                 0
    Zero Network Redirects    :                 0
    Last Resort Redirects     :                 0
----- SR Proximity Routing Statistics -----
    Cache Hits                :                 1
    Cache Misses              :                 1
    Errors                    :                 0
```

The following example shows how to display the Service Router information on the SE:

```
ServiceEngine# show service-router service-monitor
Monitor types configured:
-------------------------
CPU,MEM,KMEM,WEB,DISK,NIC

Threshold values configured:
----------------------------
CPU          : 80%
MEM          : 80%
KMEM         : 50%
NIC          : 90%
BURST COUNT : 1
```

```
DISK        : 80%
DISKFAILCNT : 1

Sample periods configured:
--------------------------
CPU  : 1 (secs)
MEM  : 1 (secs)
KMEM : 1 (secs)
NIC  : 3 (secs)
DISK : 1 (secs)

Sample counts configured to use in calculating average:
-------------------------------------------------------
CPU  : 2
MEM  : 2
KMEM : 2
NIC  : 2
DISK : 2

Device Status
-------------

CPU
Current load          : 35%
Average load          : 35%
Threshold             : Not reached

DISK
Current load          : 20%
Average load          : 20%
Threshold             : Not reached
Status                : Operational

MEM
Average Used Memory   : 10%
Threshold             : Not reached

KMEM
Average Kernel Memory : 1%
Threshold             : Not reached

NIC
Interface             : PortChannel 1/0
Average BW In         : 9%
Average BW Out        : 9%
Threshold             : Not reached

Average Device load   : 35%

Services Status
---------------

Critical Service(s)   : Running

WEB
Enabled               : Yes
Threshold             : Not reached
Stopped               : No
```

The following example shows how to display the Service Router information on the VOSM:

```
VOSM# show service-router service-monitor
Alarm types configured:
-----------------------
```

```
AUGMENTATION ALARM : Disabled

Monitor types configured:
-------------------------
CPU,MEM,KMEM,DISK

Threshold values configured:
----------------------------
CPU         : 80%
MEM         : 80%
KMEM        : 50%
DISK        : 80%
DISKFAILCNT : 75%
AUGMENTATION: 80%

Sample periods configured:
--------------------------
CPU  : 1 (secs)
MEM  : 1 (secs)
KMEM : 1 (secs)
DISK : 1 (secs)

Sample counts configured to use in calculating average:
-------------------------------------------------------
CPU  : 2
MEM  : 2
KMEM : 2
DISK : 2

Device Status
-------------

CPU
Current load          : 1%
Average load          : 1%
Threshold             : Not reached

DISK
Current load               : 1%
Average load               : 0%
Load Threshold             : Not reached
Disk Fail Cnt Threshold    : Not reached

MEM
Average Used Memory   : 6%
Threshold             : Not reached

KMEM
Average Kernel Memory : 0%
Threshold             : Not reached


Average Device load   : 1%

VOSM#
```

Related Commands

Command	Description
service-router	Configures service routing.
clear service-router	Clears the Service Router cache.

show services

To display services-related information, use the **show services** command in EXEC configuration mode.

show services {**ports** [*port_num*] | **summary**}

Syntax Description

ports	Displays services by port number.
port_num	(Optional) Displays up to eight port numbers. The port number range is from 1 to 65535.
summary	Displays the services summary.

Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to display the services information by the port number:

```
VOSM# show services ports
Service information by port
 ---------------------------
  550    Started on Mon Oct 14 12:13:20 2002
         Runs 1 service
                Cisco_Streaming_Engine
  553    Started on Mon Oct 14 12:13:20 2002
         Runs 1 service
                RTSP_Gateway
  554    Started on Mon Oct 14 12:13:20 2002
         Runs 1 service
                RTSP_Gateway
    .
    .
    .
15256    Started on Mon Oct 14 12:13:20 2002
         Runs 1 service
                CMS
27999    Started on Mon Oct 14 12:13:20 2002
         Runs 1 service
                Real_Server
28000    Started on Mon Oct 14 12:13:20 2002
         Runs 1 service
                Real_Proxy
```

The following example shows how to display a services information summary, showing the service and the associated port numbers:

```
VOSM# show services summary

             Service        Ports
-------------------------------------------------
                 CMS         15256  2000  2001  2002  2003  2004  2005
                 GUI          8001
                 icp          3128
```

```
                emdb          5432
             CertMgr          6001
           MgmtAgent          5252
          Real_Proxy          1090  8082  9002   555 28000  7879  6060  7071  3031
         VOSM_UI_http          8443
          Real_Server          7070  8081  9091 27999  7878  7802  1554  3030  4040  5050
        RTSP_Gateway           554   553
    RPC_APACHE_PORT          6550
temp_RPC_APACHE_PORT          8008
Cisco_Streaming_Engine         550 SNMP
```

show snmp

To check the status of Simple Network Management Protocol (SNMP) communications, use the **show snmp** command in EXEC configuration mode.

show snmp {**alarm-history** | **engineID** | **group** | **stats** | **user**}

Syntax Description

alarm-history	Displays SNMP alarm history information.
engineID	Displays the local SNMP engine identifier.
group	Displays SNMP groups.
stats	Displays SNMP statistics.
user	Displays SNMP users.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

This command provides information on various SNMP variables and statistics on SNMP operations.

Table 2-39 describes the fields shown in the **snmp alarm-history** display.

Table 2-39 show snmp alarm-history Field Descriptions

Field	Description
Index	Serial number of the listed alarms.
Type	Status of whether the alarm has been Raised or Cleared.
Sev	Levels of alarm severity (Critical, Major or Minor).
Alarm ID	Traps sent by a VDS-OS device contain numeric alarm IDs.
ModuleID	Traps sent by a VDS-OS device contain numeric module IDs. See Table 2-40 to map module names to module IDs.
Category	Traps sent by a VDS-OS device contain numeric category IDs. See Table 2-41 to map category names to category IDs.
Descr	Description of the VDS-OS software alarm and the application that generated the alarm.

Table 2-40 describes the mapping of module names to module IDs.

Table 2-40 Mapping of Module Names to Module IDs

Module Name	Module ID
acquirer	4000
AD_DATABASE	8000
cms	3000
MULTICAST_DATA_SENDER	7000
NHM	1
NHM/NHM	2500
nodemgr	2000
standby	4000
sysmon	1000
UNICAST_DATA_RECEIVER	5000
UNICAST_DATA_SENDER	6000

Table 2-41 describes the mapping of category names to category IDs.

Table 2-41 Mapping of Category Names to Category IDs

Category Name	Category ID
Communications	1
Service Quality	2
Processing Error	3
Equipment	4
Environment	5
Content	6

Table 2-42 describes the fields shown in the **show snmp stats** display.

Table 2-42 show snmp stats Field Descriptions

Field	Description
SNMP packets input	Total number of SNMP packets input.
Bad SNMP version errors	Number of packets with an invalid SNMP version.
Unknown community name	Number of SNMP packets with an unknown community name.
Illegal operation for community name supplied	Number of packets requesting an operation not allowed for that community.
Encoding errors	Number of SNMP packets that were improperly encoded.
Number of requested variables	Number of variables requested by SNMP managers.
Number of altered variables	Number of variables altered by SNMP managers.

Table 2-42 show snmp stats Field Descriptions (continued)

Field	Description
Get-request PDUs	Number of GET requests received.
Get-next PDUs	Number of GET-NEXT requests received.
Set-request PDUs	Number of SET requests received.
SNMP packets output	Total number of SNMP packets sent by the router.
Too big errors	Number of SNMP packets that were larger than the maximum packet size.
Maximum packet size	Maximum size of SNMP packets.
No such name errors	Number of SNMP requests that specified a Management Information Base (MIB) object that does not exist.
Bad values errors	Number of SNMP SET requests that specified an invalid value for a MIB object.
General errors	Number of SNMP SET requests that failed because of some other error. (It was not a No such name error, Bad values error, or any of the other specific errors.)
Response PDUs	Number of responses sent in reply to requests.
Trap PDUs	Number of SNMP traps sent.

Table 2-43 describes the fields shown in the **show snmp engineID** display.

Table 2-43 show snmp engineID Field Descriptions

Field	Description
Local SNMP Engine ID	String that identifies the copy of SNMP on the local device.

Table 2-44 describes the fields shown in the **show snmp group** display.

Table 2-44 show snmp group Field Descriptions

Field	Description
groupname	Name of the SNMP group, or collection of users who have a common access policy.
security_model	Security model used by the group (v1, v2c, or v3).
readview	String identifying the read view of the group.
writeview	String identifying the write view of the group.
notifyview	String identifying the notify view of the group.

Table 2-45 describes the fields shown in the **show snmp user** display.

Table 2-45 show snmp user Field Descriptions

Field	Description
User name	String identifying the name of the SNMP user.
Engine ID	String identifying the name of the copy of SNMP on the device.
Group Name	Name of the SNMP group, or collection of users who have a common access policy.

Related Commands

Command	Description
snmp-server community	Configures the community access string to permit access to the SNMP.
snmp-server contact	Sets the system server contact (sysContact) string.
snmp-server enable traps	Enables the Service Engine (SE) to send SNMP traps.
snmp-server group	Defines a user security model group.
snmp-server host	Specifies the recipient of a host SNMP trap operation.
snmp-server location	Sets the SNMP system location string.
snmp-server notify inform	Configures the SNMP notify inform request.
snmp-server user	Defines a user who can access the SNMP server.
snmp-server view	Defines a SNMP V2 MIB view.

show ssh

To display Secure Shell (SSH) status and configuration information, use the **show ssh** command in EXEC configuration mode.

show ssh

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Related Commands

Command	Description
sshd	Enables the SSH daemon.

show standby

To display standby interface information, use the **show standby** command in EXEC configuration mode.

show standby

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-46 describes the fields shown in the **show standby** display.

Table 2-46 show standby Field Descriptions

Field	Description
Standby Group	Number that identifies the standby group.
Description	Description of the device, as configured by using the **description** option of the **interface** global configuration command.
IP address	IP address of the standby group.
netmask	Netmask of the standby group.
Member interfaces	Member interfaces of the standby group. Shows which physical interfaces are part of the standby group. Shows the interface definition, such as GigabitEthernet 1/0.
priority	Priority status of each interface.
Active interface	Interfaces that are currently active in the standby group.
Maximum errors allowed on the active interface	Maximum number of errors allowed on the active interface.

Related Commands

Command	Description
show interface	Displays the hardware interface information.
show running-config	Displays the current running configuration information on the terminal.
show startup-config	Displays the startup configuration.

show startup-config

To display the startup configuration, use the **show startup-config** command in EXEC configuration mode.

show startup-config

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use this command to display the configuration used during an initial bootup, stored in non-volatile random-access memory (NVRAM).

Examples

The following example shows how to display the startup configuration details on the SE:

```
ServiceEngine# show startup-config
! VDS-OS version 2.3.9
!
device mode service-engine
!
hostname V2-CDE220-3
!
primary-interface PortChannel 1
!
interface PortChannel 1
 ip address 3.1.14.72 255.255.255.0
 exit
interface PortChannel 2
 ip address 4.0.8.13 255.255.255.0
 exit
!
interface GigabitEthernet 1/0
 channel-group 2
 exit
interface GigabitEthernet 2/0
 channel-group 2
 exit
interface GigabitEthernet 3/0
 channel-group 1
 exit
interface GigabitEthernet 4/0
 channel-group 1
 exit
interface GigabitEthernet 5/0
 channel-group 1
 exit
interface GigabitEthernet 6/0
 channel-group 1
```

```
 exit
!
ip default-gateway 3.1.14.1
!
offline-operation enable
!
rule action block pattern-list 3
rule action redirect http://www.baidu.com pattern-list 2
rule pattern-list 1 url-regex http://chunliu.com/b.wmv
rule pattern-list 2 header-field request-line b.wmv
rule pattern-list 3 header-field request-line c.wmv
!
icap service camiant
  server icap://trythis/servername
  exit
!
transaction-logs enable
transaction-logs archive interval 120
!
username admin password 1 bVmDmMMmZAPjY
username admin privilege 15
!
authentication login local enable primary
authentication configuration local enable primary
!
access-lists 300 deny groupname Disney
access-lists 300 permit groupname any
access-lists enable
!
telnet enable
!
VOSM ip 4.0.8.10
cms enable
!
cache content max-cached-entries 1000
! End of VDS-OS configuration
```

Related Commands

Command	Description
configure	Enters global configuration mode.
copy	Copies the configuration or image data from a source to a destination.
show running-config	Displays the current running configuration information on the terminal.

show statistics access-lists

To display SE access control list statistics, use the **show statistics access-lists** command in EXEC configuration mode.

show statistics access-lists

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The access control list statistics display the number of access requests, denials, and permissions recorded. Use the **show statistics access-lists 300** command to display the number of group name accesses recorded.

Table 2-47 describes the fields shown in the **show statistics access-lists 300** display.

Table 2-47 show statistics access-lists 300 Field Descriptions

Field	Description
Access Control Lists Statistics	
Groupname and username-based List	Lists the group name-based access control lists.
Number of requests	Number of requests.
Number of deny responses	Number of deny responses.
Number of permit responses	Number of permit responses.

Related Commands

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.

show statistics admission

To display admission control statistics, use the **show statistics admission** command in EXEC configuration mode.

show statistics admission

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-48 describes the fields shown in the **show statistics admission** display.

Table 2-48 show statistics admission

Field	Description
QOS Admission Check	
Bypassed	
Attempts	
Succeeded	
Failed	
Best effort	
Attempts	
Based on congestion	
Succeeded	
Failed	
Too many sessions	
Average too low	
Soft guaranteed	
Attempts	
Succeeded	
Failed	
Disk congestion	

Table 2-48 show statistics admission (continued)

Field	Description
BE would be too low	
Over threshold	
Hard guaranteed	
Attempts	
Succeeded	
Failed	
Hole management	
Bypassed	
Succeeded	
Failed	
fill too close	
Hit data	
with active fill	
request range inside inactive fill	
request range overlaps inactive fill	
Hit hole	
not aligned, 2 fills	
aligned, 1 fill	
too many fills	
too many holes	
fill from start	
active fill	
fill from left	
Disk overload	
Misc errors	

show statistics cdnfs

To display SE CDS network file system (cdnfs) statistics, use the **show statistics cdnfs** command in EXEC configuration mode.

show statistics cdnfs

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-49 describes the **show statistics cdnfs** command fields displayed in the command output.

Table 2-49 show statistics cdnfs Fields

Field	Description
Size of physical file system	Physical disk size of the CDS network file system (CDNFS).
Space assigned for cdnfs purposes	Amount of physical disk space on the CDNFS that has been assigned to hold prepositioned objects. The space can be less than the size of the file system.
Number of cdnfs entries	Number of CDNFS objects. **Note** One prepositioned file internally uses two CDNFS entries. The number of CDNFS entries is twice the number of actual files displayed to users.
Space reserved for cdnfs entries	Amount of disk space reserved for existing prepositioned objects. This space is reserved for CDNFS objects before the file is created and written to the file system.
Available space for new entries	Amount of physical disk space available in the CDNFS for new prepositioned objects.
Physical file system in use	Amount of physical disk space currently in use by the CDNFS.
Physical file system space free	Amount of unused physical disk space in the CDNFS
Physical file system percentage in use	Percentage of physical disk space in use relative to the total disk space available.

Related Commands

Command	Description
cdnfs	Manages the Internet Streamer CDNFS.
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.

Command	Description
show cdnfs	Displays CDNFS information.
show disks	Displays the names of the disks currently attached to the SE.

show statistics content-mgr

To display Content Manager statistics, use the **show statistics content-mgr** command in EXEC configuration mode.

show statistics content-mgr

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-50 describes the **show statistics content-mgr** command fields displayed in the command output.

Table 2-50 show statistics content-mgr Fields

Field	Description
Add Message Count	Counter to track when new content is added in content manager. The source of content can be either protocol engine or snapshot.
Update Message Count	Counter to track when content is updated in content manager.
Delete Message Count	Counter to track when content is deleted in content manager.
New Content Count	Counter to track when new content is added in content manager from protocol engine. This does not include content added via snapshot.
Slow Scan Cache Count	Count of cached content added to content manager via slow scan
Slow Scan Preposition Count	Count of preposition content added to content manager via slow scan.
Last Slow Scan Time	Time at which last slow scan operation was performed.
Snapshot Recovered Count	Counter to track when new content is added to content manager from snapshot. This does not include content added via protocol engine.
Deletion Task Count	Number of deletion tasks in Content Manager.
Evicted Asset Count	Count of assets evicted.
Eviction count Disk Size	Number of evictions occurred due to insufficient disk size.
Last Eviction Time	Last time at which eviction added.
Eviction Protect Add Count	Number of contents added for eviction protection.
Eviction Protect Delete Count	Number of contents removed from eviction protection.
Eviction Protect Skip Count	Number of contents skipped since it is protected by eviction protection.

Table 2-50 show statistics content-mgr Fields (continued)

Field	Description
Deletion Store Size	Count of entries present in deletion store.
Preposition Asset Count	Count of preposition assets.
Cache Asset Count	Count of cache assets.
Preposition Asset Size	Disk size for preposition assets.
Cache Asset Size	Disk size for cache assets.
Total Asset Size	Total size for preposition and cache assets.
Current Memory Usage	Current memory usage of Content Manager process.
Slow Scan In Progress	Is slow scan process running?
Clear-Cache-All Count	Number of times cache was cleared by clear all command.
Deletion In Progress	Is content deletion currently in progress?
Snapshot In Progress	Is Snapshot writer running?
Snapshot Reader up	Is Snapshot reader running?
Priority Queue Size	Number of assets present in priority queue/.
Eviction Protection Size	Number of entries present in eviction protection table.
Eviction Count-Mem Usage	Number of evictions occurred due to less mem usage.
Eviction Count-Content Count	Number of evictions due max content limit reached.
Eviction Protect Max Size	Max size of the eviction protection table since start of content manager.
Last Cache Clear Time	Time at which cache was cleared.
Last Statistics Clear Time	Time at which statistics was cleared.
Last Global Eviction Time	Time at which global eviction happened.

Related Commands-

Command	Description
contentmgr	Configures the Content Manager.
content-mgr disk-info force-reset	Forces the Content Manager to reset the disk share memory information.
show content-mgr	Displays all content management information.

show statistics fd

To display file descriptors limit statistics, use the **show statistics netstat** command in EXEC configuration mode.

show statistics fd

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-57 describes the fields shown in the **show statistics fd** display.

Table 2-51 show statistics netstat Field Descriptions

Field	Description
Number of file descriptors in use	Displays the number of file descriptions currently in use.
Maximum number of file descriptions allowed	Displays the maximum number of file descriptions allowed at one time.
Percentage of file descriptions in use	Displays the percentage of file descriptions currently in use.

Examples

The following is sample output from the **show statistics fd** command:

```
ServiceEngine# show statistics fd
Number of file descriptors in use            = 3600
Maximum number of file descriptions allowed  = 262144
Percentage of file descriptions in use       = 1.37%
```

show statistics icmp

To display SE Internet Control Message Protocol (ICMP) statistics, use the **show statistics icmp** command in EXEC configuration mode.

show statistics icmp

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

ICMP messages are sent in several situations, such as when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route. The purpose of these control messages is to provide feedback about problems in the communication environment, not to make IP reliable. There is still no guarantee that a datagram is delivered or a control message is returned. Some datagrams may still be undelivered without any report of their loss.

The ICMP messages typically report errors in the processing of datagrams. To avoid the infinite regress of messages about messages, no ICMP messages are sent about ICMP messages. Also, ICMP messages are only sent about errors in handling fragment zero of fragmented datagrams.

ICMP messages are sent using the basic IP header. The first octet of the data portion of the datagram is on a ICMP type field; the value of this field determines the format of the remaining data.

Many of the type fields contain more specific information about the error condition identified by a code value. ICMP messages have two types of codes:

- Query
- Error

Queries contain no additional information because they ask for information and show a value of 0 in the code field. ICMP uses the queries as shown in Table 2-52.

Table 2-52 Queries

Query	Type Field Value
Echo Reply	0
Echo Request	8
Router Advertisement	9
Router Solicitation	10
Time-stamp Request	13
Time-stamp Reply	14
Information Request (obsolete)	15

Table 2-52 Queries (continued)

Query	Type Field Value
Information Reply (obsolete)	16
Address Mask Request	17
Address Mask Reply	18

Error messages give specific information and have varying values that further describe conditions. Error messages always include a copy of the offending IP header and up to 8 bytes of the data that caused the host or gateway to send the error message. The source host uses this information to identify and fix the problem reported by the ICMP error message. ICMP uses the error messages as shown in Table 2-53.

Table 2-53 Errors

Error	Type Field Value
Destination Unreachable	3
Source Quench	4
Redirect	5
Time Exceeded	11
Parameter Problems	12

Table 2-54 describes the fields shown in the **show statistics icmp** display.

Table 2-54 show statistics icmp Field Descriptions

Field	Description
ICMP messages received	Total number of ICMP messages received by the SE.
ICMP messages receive failed	Total number of ICMP messages that were not received by the SE.
Destination unreachable	Number of destination-unreachable ICMP packets received by the SE. A destination-unreachable message (Type 1) is generated in response to a packet that cannot be delivered to its destination address for reasons other than congestion. The reason for the nondelivery of a packet is described by the code field value. Destination-unreachable packets use the code field values to further describe the function of the ICMP message being sent.

Table 2-54 show statistics icmp Field Descriptions (continued)

Field	Description
Timeout in transit	Number of ICMP time-exceeded packets received by the SE. The time-exceeded message occurs when a router receives a datagram with a Time-to-Live (TTL) of 0 or 1. IP uses the TTL field to prevent infinite routing loops. A router cannot forward a datagram that has a TTL of 0 or 1. Instead, it trashes the datagram and sends a time-exceeded message. Two different time-exceeded error codes can occur, as follows: • 0 = Time-To-Live Equals 0 During Transit • 1 = Time-To-Live Equals 0 During Reassembly A router cannot forward a datagram with a TTL of 0 or 1 both during transit or reassembly. The TTL timer is measured, in seconds, and originally was used before the existence of routers to guarantee that a datagram did not live on the Internet forever. Each gateway processing a datagram reduces this value by at least one if it takes longer to process and forward the datagram. When this value expires, the gateway trashes the datagram and sends a message back to the sender notifying the host of the situation.
Wrong parameters	Number of ICMP packets with parameter problems received by the SE. An IP datagram that has been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 12 denote a parameter problem on a datagram. ICMP parameter-problem datagrams are issued when a router has had to drop a malformed datagram. This condition is a normal and necessary type of network traffic; however, large numbers of this datagram type on the network can indicate network difficulties or hostile actions. A host or gateway can send this message when no other ICMP message covering the problem can be used to alert the sending host.
Source quenches	Number of ICMP source-quench packets received by the SE. A receiving host generates a source-quench message when it cannot process datagrams at the speed requested because of a lack of memory or internal resources. This message serves as a simple flow control mechanism that a receiving host can use to alert a sender to slow down its data transmission. When the source host receives this message, it must pass this information on to the upper-layer process, such as TCP, which then must control the flow of the application's data stream. A router generates this message when, in the process of forwarding datagrams, it has run low on buffers and cannot queue the datagram for delivery.

Table 2-54 show statistics icmp Field Descriptions (continued)

Field	Description
Redirects	Number of ICMP redirect packets received by the SE. A router sends a redirect error to the sender of an IP datagram when the sender should have sent the datagram to a different router or directly to an end host (if the end host is local). The message assists the sending host to direct a misdirected datagram to a gateway or host. This alert does not guarantee proper delivery; the sending host has to correct the problem if possible. Only gateways generate redirect messages to inform source hosts of misguided datagrams. A gateway receiving a misdirected frame does not trash the offending datagram if it can forward it.
Echo requests	Number of echo ICMP packets received by the SE. An echo request is an IP datagram that has been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 8. The ICMP echo request is issued by the source to determine if the destination is alive. When the destination receives the request, it replies with an ICMP echo reply. This request and reply pair is most commonly implemented using the ping utility. Many network management tools use this utility or some derivative of it, and this condition is common as a part of network traffic. **Note** You should be suspicious when a large number of these packets are found on the network.
Echo replies	Number of echo-reply ICMP packets received by the SE. An echo reply is the message that is generated in response to an echo request message. An echo reply is an IP datagram that has been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 0. This condition is common as a part of network traffic. **Note** You should be suspicious when a large number of these packets are found on the network.
Timestamp requests	Number of ICMP time stamp request packets received by the SE. An ICMP time stamp request is an IP datagram that has been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 13. The ICMP time stamp request and reply pair can be used to synchronize system clocks on the network. The requesting system issues the time stamp request bound for a destination, and the destination system responds with a time stamp reply message. This condition is normal as a part of network traffic but is uncommon on most networks. **Note** You should be suspicious when a large number of these packets are found on the network.

Table 2-54 show statistics icmp Field Descriptions (continued)

Field	Description
Timestamp replies	Number of ICMP time stamp reply packets received by the SE. time stamp request and reply messages work in tandem. You have the option of using time stamps. When used, a time stamp request permits a system to query another for the current time. It expects a recommended value returned to be the number of milliseconds since midnight, Coordinated Universal Time (UTC). This message provides millisecond resolution. The two systems compare the three time stamps and use a round-trip time to adjust the sender's or receiver's time if necessary. Most systems set the transmit and receive time as the same value.
Address mask requests	Number of ICMP address mask request packets received by the SE. An ICMP address mask request is an IP datagram that has been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 17. ICMP address mask requests could be used to perform reconnaissance sweeps of networks. The ICMP address mask request and reply pair can be used to determine the subnet mask used on the network. When the requesting system issues the address mask request bound for a destination, the destination system responds with an address mask reply message. This condition can be a part of normal network traffic but is uncommon on most networks. **Note** You should be suspicious when a large number of these packets are found on the network.
Address mask replies	Number of ICMP address mask reply packets received by the SE. An address mask ICMP reply is an IP datagram that has been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 18. No known exploits incorporate this option. The ICMP address mask request and reply pair can be used to determine the subnet mask used on the network. When the requesting system issues the address mask request bound for a destination, the destination system responds with an address mask reply message. This condition can be a part of normal network traffic but is uncommon on most networks. **Note** You should be suspicious when a large number of these packets are found on the network.
ICMP messages sent	Total number of ICMP messages sent by the SE.
ICMP messages send failed	Total number of ICMP messages that failed to be sent by the SE.
Destination unreachable	Number of destination-unreachable ICMP packets sent by the SE.
Timeout in transit	Number of ICMP time-exceeded packets sent by the SE.
Wrong parameters	Number of ICMP packets with parameter problems sent by the SE.
Source quenches	Number of ICMP source-quench packets sent by the SE.
Redirects	Number of ICMP redirect packets sent by the SE.
Echo requests	Number of echo ICMP packets sent by the SE.

Table 2-54 show statistics icmp Field Descriptions (continued)

Field	Description
Echo replies	Number of echo-reply ICMP packets sent by the SE.
Timestamp requests	Number of ICMP time stamp request packets sent by the SE.
Timestamp replies	Number of ICMP time stamp reply packets sent by the SE.
Address mask requests	Number of ICMP address mask requests sent by the SE.
Address mask replies	Number of ICMP address mask replies sent by the SE.

Related Commands

Command	Description
clear statistics	Clears the statistics settings.

show statistics icmpv6

To display the Internet Control Message Protocol (ICMP) v6 statistics, use the **show statistics icmpv6** command in user EXEC configuration mode.

show statistics icmpv6

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

User EXEC configuration mode.

Examples

The following is sample output from the **show statistics icmpv6** command:

```
ServiceRouter# show statistics icmpv6

ICMPv6 statistics
---------------
ICMPv6 messages received         = 0
ICMPv6 messages receive failed   = 0
 Destination unreachable         = 0
 Packet too big                  = 0
 Timeout in transit              = 0
 Wrong parameters                = 0
 Echo requests                   = 0
 Echo replies                    = 0
 Group member queries            = 0
 Group member responses          = 0
 Group member reductions         = 0
 Router solicits                 = 0
 Router advertisements           = 0
 Neighbor solicits               = 0
 Neighbor advertisements         = 0
 Redirects                       = 0
 MLDv2 reports                   = 0
ICMPv6 messages sent             = 0
 Destination unreachable         = 0
 Packet too big                  = 0
 Time exceeded                   = 0
 Wrong parameters                = 0
 Echo requests                   = 0
 Echo replies                    = 0
 Group member queries            = 0
 Group member responses          = 0
 Group member reductions         = 0
 Router solicits                 = 0
 Router advertisements           = 0
 Neighbor solicits               = 0
 Neighbor advertisements         = 0
 Redirects                       = 0
 MLDv2 reports                   = 0
```

Table 2-56 describes the fields shown in the **show statistics icmpv6** display.

Table 2-55 show statistics icmpv6 Field Descriptions

Field	Description
ICMPv6 messages received	
ICMPv6 messages receive failed	
Destination unreachable	
packet too big	
Timeout in transit	
Wrong parameters	
Echo requests	
Echo replies	
Group member queries	
Group member responses	
Group member reductions	
Router solicits	
Router advertisements	
Neighbor solicits	
Neighbor advertisements	
Redirects	
MLDv2 reports	
ICMPv6 messages receive sent	
Destination unreachable	
packet too big	
Timeout in transit	
Wrong parameters	
Echo requests	
Echo replies	
Group member queries	
Group member responses	
Group member reductions	
Router solicits	
Router advertisements	
Neighbor solicits	
Neighbor advertisements	
Redirects	
MLDv2 reports	

Related Commands

Command	Description
clear statistics icmpv6	Clears Icmpv6 statistics counters.

show statistics ip

To display the IP statistics, use the **show statistics ip** command in user EXEC configuration mode.

show statistics ip

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

User EXEC configuration mode.

Examples

The following is sample output from the **show statistics ip** command:

```
ServiceRouter# show statistics ip

IP statistics
-------------
Total packets in                = 1408126
 with invalid header            = 0
 with invalid address           = 0
 forwarded                      = 0
 unknown protocol               = 0
 discarded                      = 0
 delivered                      = 1408126
Total packets out               = 1500110
 dropped                        = 0
 dropped (no route)             = 0
Fragments dropped after timeout  = 0
Reassemblies required           = 0
Packets reassembled             = 0
Packets reassemble failed       = 0
Fragments received              = 0
Fragments failed                = 0
Fragments created               = 0

ServiceRouter#
```

Table 2-56 describes the fields shown in the **show statistics ip** display.

Table 2-56 show statistics ip Field Descriptions

Field	Description
Total packets in	Total number of input datagrams received from interfaces, including those received in error.
with invalid header	Number of input datagrams discarded because of errors in their IP headers, including bad checksums, version number mismatch, other format errors, Time To Live exceeded, errors discovered in processing their IP options, and so on.

Table 2-56 show statistics ip Field Descriptions (continued)

Field	Description
with invalid address	Number of input datagrams discarded because the IP address in the IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported classes (for example, Class E). For entities that are not IP routers and do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
forwarded	Number of input datagrams for which this entity was not the final IP destination, but the SE attempted to find a route to forward them to that final destination. In entities that do not act as IP routers, this counter includes only those packets that were source-routed through this entity, and the source-route option processing was successful.
unknown protocol	Number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
discarded	Number of input IP datagrams that were discarded even though the datagrams encountered no problems to prevent their continued processing. This counter does not include any datagrams discarded while awaiting reassembly.
delivered	Total number of input datagrams successfully delivered to IP user protocols (including ICMP).
Total packets out	Total number of IP datagrams that local IP user protocols (including ICMP) supplied to IP in requests for transmission. This counter does not include any datagrams counted in the forwarded field.
dropped	Number of output IP datagrams that were discarded even though the datagrams encountered no problems that would prevent their transmission to their destination. This counter would include datagrams counted in the forwarded field if any such packets met this (discretionary) discard criterion.
dropped (no route)	Number of IP datagrams that were discarded because the SE found no route to send them to their destination. This counter includes any packets counted in the forwarded field that meet this no-route criterion including any datagrams that a host cannot route because all its default routers are down.
Fragments dropped after timeout	Number of received fragments at this entity that are dropped after being held for the maximum number of seconds while awaiting reassembly at this entity.
Reassemblies required	Number of IP fragments received that needed to be reassembled at this entity.
Packets reassembled	Number of IP datagrams successfully reassembled.

Table 2-56 show statistics ip Field Descriptions (continued)

Field	Description
Packets reassemble failed	Number of failures detected by the IP reassembly algorithm (because of reasons such as timed out and errors.) This counter is not necessarily a count of discarded IP fragments because some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
Fragments received	Number of IP datagrams that have been successfully fragmented at this entity.
Fragments failed	Number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be fragmented for reasons such as the Don't Fragment flag was set.
Fragments created	Number of IP datagram fragments that have been generated because of fragmentation at this entity.

Related Commands

Command	Description
clear statistics ip	Clears IP statistics counters.
ip	Configures the IP.
show ip routes	Displays the IP routing table.

show statistics lsof

To display the List of Open File (lsof) descriptors, use the **show statistics lsof** command in EXEC configuration mode.

show statistics lsof

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows to display the lsof descriptors:

```
ServiceEngine# show statistics lsof
COMMAND     PID     USER   FD      TYPE             DEVICE     SIZE       NODE
NAME
init          1    admin  cwd       DIR               1,0     1024          2
/
init          1    admin  rtd       DIR               1,0     1024          2
/
init          1    admin  txt       REG               1,0    45436       7488
/sbin/init
init          1    admin  mem       REG               1,0  1852502       6566
/lib/libc-2.13.so
init          1    admin  mem       REG               1,0   154528       2006
/lib/ld-2.13.so
init          1    admin  10u      FIFO              0,13                4069
/dev/initctl
kthreadd      2    admin  cwd       DIR               1,0     1024          2
/
kthreadd      2    admin  rtd       DIR               1,0     1024          2
/
kthreadd      2    admin  txt   unknown
/proc/2/exe
migration     3    admin  cwd       DIR               1,0     1024          2
/
migration     3    admin  rtd       DIR               1,0     1024          2
/

<Output truncated>
```

show statistics netstat

To display SE Internet socket connection statistics, use the **show statistics netstat** command in EXEC configuration mode.

show statistics netstat

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-57 describes the fields shown in the **show statistics netstat** display.

Table 2-57 show statistics netstat Field Descriptions

Field	Description
Proto	Layer 4 protocol used on the Internet connection, such as TCP, UDP, and so forth.
Recv-Q	Amount of data buffered by the Layer 4 protocol stack in the receive direction on a connection.
Send-Q	Amount of data buffered by the Layer 4 protocol stack in the send direction on a connection.
Local Address	IP address and Layer 4 port used at the device end point of a connection.
Foreign Address	IP address and Layer 4 port used at the remote end point of a connection.
State	Layer 4 state of a connection. TCP states include the following: ESTABLISHED, TIME-WAIT, LAST-ACK, CLOSED, CLOSED-WAIT, SYN-SENT, SYN-RCVD, SYN-SENT, SYN-ACK-SENT, and LISTEN.

show statistics radius

To display SE RADIUS authentication statistics, use the **show statistics radius** command in EXEC configuration mode.

show statistics radius

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The fields in the **show statistics radius** display are as follows:

- Number of access requests
- Number of access deny responses
- Number of access allow responses
- Number of authorization requests
- Number of authorization failure responses
- Number of authorization success responses

Related Commands

Command	Description
clear statistics	Clears the statistics settings.
radius-server	Configures the RADIUS authentication.
show radius-server	Displays the RADIUS server information.

show statistics service-router

To display Service Router statistics, use the **show statistics service-router** command in EXEC configuration mode.

show statistics service-router {**all** | **content-origin** *content_name* | **dns** | **history** | **keepalive** | **routing**} | **se** *se_name* | **summary**}

Syntax Description

all	Displays all statistics.
content-origin	Displays content origin specific statistics.
content_name	Content origin name to show.
dns	Displays Domain Name System (DNS) statistics.
history	Displays statistics history.
keepalive	Displays keepalive statistics.
routing	Displays routing statistics.
se	Displays Service Engine specific statistics.
se_name	Service Engine name to show.
summary	Displays summary statistics.

Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to display the content origin-specific statistics on the number of requests and redirects:

```
ServiceRouter# show statistics service-router content-origin

----- SR Statistics Of Content Origin -----
domain: sr.ABC.com (Origin Services: ABC.com)
HTTP Requests (normal) :                    0
HTTP Requests (ASX)    :                    0
HTTP Requests (API)    :                    0
RTSP Requests          :                    0
RTMP Requests          :                    0
HTTP 302 Redirects     :                    0
ASX Redirects          :                    0
HTTP API Redirects     :                    0
RTSP Redirects         :                    0
RTMP Redirects         :                    0
Overflow Redirects     :                    0

----- SR Statistics Of Content Origin -----
domain: chunliu.com (Origin Services: 72.163.255.111)
HTTP Requests (normal) :                    0
HTTP Requests (ASX)    :                    0
HTTP Requests (API)    :                    0
RTSP Requests          :                    0
```

```
RTMP Requests          :                    0
HTTP 302 Redirects     :                    0
ASX Redirects          :                    0
HTTP API Redirects     :                    0
RTSP Redirects         :                    0
RTMP Redirects         :                    0
Overflow Redirects     :                    0

----- SR Statistics Of Content Origin -----
domain: install3.com (Origin Services: 10.74.115.24)
HTTP Requests (normal) :                    0
HTTP Requests (ASX)    :                    0
HTTP Requests (API)    :                    0
RTSP Requests          :                    0
RTMP Requests          :                    0
HTTP 302 Redirects     :                    0
ASX Redirects          :                    0
HTTP API Redirects     :                    0
RTSP Redirects         :                    0
RTMP Redirects         :                    0
Overflow Redirects     :                    0
V2-CDE220-2#
```

The following example shows how to display the DNS statistics, including the number of DNS queries for each type (Content Origin FQDN, Service Engine aliases), and the response sent (aliases for down Service Engines, unknown domains, failed, dropped).

:

```
ServiceRouter# show statistics service-router dns

----- SR DNS Statistics -----
Total DNS queries             :                 0
    Content Origin FQDNs      :                 0
    Service Engine aliases    :                 0
    Aliases for Down SEs      :                 0
    Unknown domains           :                 0
    PTR queries               :                 0
    Failed                    :                 0
    Dropped                   :                 0

ServiceRouter#
```

The following example shows how to display the statistics history on the number of redirect requests (maximum, minimum, average, last [in the past hour or minute]):

```
ServiceRouter# show statistics service-router history

----- SR Statistics History -----
Type         Minimum   Maximum   Average      Last (in past hour/per minute)
---------- --------- --------- --------- ---------
REQUESTS           0         0         0         0
REDIRECTS          0         0         0         0
```

The following example shows how to display keepalive statistics on the number of keepalives received from Service Engines, unknown source, and number of keepalives dropped:

```
ServiceRouter# show statistics service-router keepalive

----- SR Keepalive Statistics -----
    Dropped                   :                 0
    Service Engine keepalives :                 0
    From unknown source       :                 0
```

```
ServiceRouter#
```

The following example shows how to display statistics to show which routing method is used in redirection to SEs:

```
ServiceRouter# show statistics service-router routing

----- SR Routing Statistics -----
    Network Redirects         :                 0
    Proximity Redirects       :                 0
    Geo Location Redirects    :                 4
    Zero Network Redirects    :                 0
    Last Resort Redirects     :                 1

ServiceRouter#
```

The following example shows how to display proximity-related statistics showing the number of cache hits, cache misses and errors.

```
ServiceRouter# show statistics service-router routing proximity

----- SR Proximity Routing Statistics -----
    Cache Hits                :                 2
    Cache Misses              :                 3
    Errors                    :                 2

ServiceRouter#
```

The following example shows how to display Service Engine statistics including liveness of the SE, number of redirects to that particular SE, and the total number of keepalives received from that SE.

```
ServiceRouter# show statistics service-router se

----- Statistics Of SE: V2-CDE220-1 -----
Aliveness               : down
HTTP 302 Redirects      :                  0
ASX Redirects           :                  0
HTTP API Redirects      :                  0
RTSP Redirects          :                  0
RTMP Redirects          :                  0
DNS Redirects           :                  0
Number Of Keepalives    :                  0

----- Statistics Of SE: V2-CDE220-3 -----
Aliveness               : down
HTTP 302 Redirects      :                  0
ASX Redirects           :                  0
HTTP API Redirects      :                  0
RTSP Redirects          :                  0
RTMP Redirects          :                  0
DNS Redirects           :                  0
Number Of Keepalives    :                  0
V2-CDE220-2#
```

The following example shows how to display summary statistics including the number of requests received, requests redirected, requests served, and requests not redirected:

```
ServiceRouter# show statistics service-router summary

----- SR Summary Statistics -----
Requests Received          :                  1
  HTTP Requests (normal)   :                  0
  HTTP Requests (ASX)      :                  0
```

```
  HTTP Requests (API)      :                0
  RTSP Requests            :                1
  RTMP Requests            :                0
  DNS Requests             :                0

Requests Served            :                0
  HTTP Requests Served     :                0

Requests Redirected        :                1
  HTTP 302 Redirects       :                0
  ASX Redirects            :                0
  HTTP API Redirects       :                0
  RTSP redirects           :                1
  RTMP redirects           :                0
  DNS redirects            :                0

Requests Overflowed        :                0
  HTTP 302 Redirects       :                0
  ASX Redirects            :                0
  HTTP API Redirects       :                0
  RTSP redirects           :                0
  RTMP redirects           :                0
  DNS redirects            :                0

Requests Not Redirected    :                0
  No SE Covering Client    :                0
  Unknown Content Origin   :                0
  Invalid Requests         :                0
  Session limit exceeded   :                0
  Bandwidth limit exceeded :                0

  "Stale SE" Requests      :                0
```

Related Commands

Command	Description
service-router	Configures service routing.
show service-router	Displays the Service Router configuration.

show statistics services

To display SE services statistics, use the **show statistics services** command in EXEC configuration mode.

show statistics services

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-58 describes the fields shown in the **show statistics services** display.

Table 2-58 show statistics services Field Descriptions

Field	Description
Port Statistics	Service-related statistics for each port on the Wide Area Applications Services (WAAS) device.
Port	Port number.
Total Connections	Number of total connections.

Related Commands

Command	Description
show services	Displays the services-related information.

show statistics snmp

To display SE Simple Network Management Protocol (SNMP) statistics, use the **show statistics snmp** command in EXEC configuration mode.

show statistics snmp

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-42 describes the fields shown in the **show statistics snmp** display.

Table 2-59 show statistics snmp Field Descriptions

Field	Description
SNMP packets input	Total number of SNMP packets input.
Bad SNMP version errors	Number of packets with an invalid SNMP version.
Unknown community name	Number of SNMP packets with an unknown community name.
Illegal operation for community name supplied	Number of packets requesting an operation not allowed for that community.
Encoding errors	Number of SNMP packets that were improperly encoded.
Number of requested variables	Number of variables requested by SNMP managers.
Number of altered variables	Number of variables altered by SNMP managers.
Get-request PDUs	Number of GET requests received.
Get-next PDUs	Number of GET-NEXT requests received.
Set-request PDUs	Number of SET requests received.
SNMP packets output	Total number of SNMP packets sent by the router.
Too big errors	Number of SNMP packets that were larger than the maximum packet size.
Maximum packet size	Maximum size of SNMP packets.
No such name errors	Number of SNMP requests that specified a Management Information Base (MIB) object that does not exist.
Bad values errors	Number of SNMP SET requests that specified an invalid value for a MIB object.

Table 2-59 show statistics snmp Field Descriptions (continued)

Field	Description
General errors	Number of SNMP SET requests that failed because of some other error. (It was not a No such name error, Bad values error, or any of the other specific errors.)
Response PDUs	Number of responses sent in reply to requests.
Trap PDUs	Number of SNMP traps sent.

Related Commands

Command	Description
show snmp	Displays the SNMP parameters.
snmp-server community	Configures the community access string to permit access to the SNMP.
snmp-server contact	Sets the system server contact string.
snmp-server enable	Enables the Service Engine (SE) to send SNMP traps.
snmp-server group	Defines a user security model group.
snmp-server host	Specifies the hosts to receive SNMP traps.
snmp-server location	Sets the SNMP system location string.
snmp-server notify inform	Configures the SNMP notify inform request.
snmp-server user	Defines a user who can access the SNMP engine.

show statistics tacacs

To display Service Engine (SE) Terminal Access Controller Access Control System Plus (TACACS+) authentication and authorization statistics, use the **show statistics tacacs** command in user EXEC configuration mode.

show statistics tacacs

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

The fields shown in the **show statistics tacacs** display for the service engine are as follows:

- Number of access requests
- Number of access deny responses
- Number of access allow responses
- Number of authorization requests
- Number of authorization failure responses
- Number of authorization success responses
- Number of accounting requests
- Number of accounting failure responses
- Number of accounting success responses

Related Commands

Command	Description
clear tacacs	Clears the TACACS+ settings.
show tacacs	Displays TACACS+ authentication protocol configuration information.
tacacs	Configures TACACS+ server parameters.

show statistics tcp

To display SE Transmission Control Protocol (TCP) statistics, use the **show statistics tcp** command in EXEC configuration mode.

show statistics tcp

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-60 describes the fields shown in the **show statistics tcp** display.

Table 2-60 show statistics tcp Field Descriptions

Field	Description
Server connection openings	Number of connections opened from the SE to the server.
Client connection openings	Number of connections opened from the client to the SE.
Failed connection attempts	Number of incoming SYN connections rejected because of rate limiting or resource shortage.
Connections established	Number of incoming connections that have been set up.
Connections resets received	Number of resets (RSTs) received by the SE.
Connection resets sent	Number of RSTs sent by the SE.
Segments received	Number of TCP segments received from the client and the server. The value of this field is almost equal to the sum of the values of the Server segments received and the Client segments received fields.
Segments sent	Number of TCP segments sent by the client and the server. The value of this field is almost equal to the sum of the values of the Server segments sent and the Client segments sent fields.
Bad segments received	Number of incoming segments dropped because of checksum or being outside the TCP window.
Segments retransmitted	Number of TCP segments retransmitted by the client and the server. The value of this field is almost equal to the sum of the values of the Server segments retransmitted and the Client segments retransmitted fields.

Table 2-60 show statistics tcp Field Descriptions (continued)

Field	Description
Retransmit timer expirations	Number of times that the TCP retransmit timer expires. The TCP sender uses a timer to measure the time that has elapsed between sending a data segment and receiving the corresponding ACK from the receiving side of the TCP transmission. When this retransmit timer expires, the sender (according to the RFC standards for TCP congestion control) must reduce its sending rate.
Server segments received	Number of TCP segments received by the SE from the server.
Server segments sent	Number of TCP segments sent by the SE to the server.
Server segments retransmitted	Number of TCP segments retransmitted by the SE from the server.
Client segments received	Number of TCP segments received by the SE from the client.
Client segments sent	Number of TCP segments sent by the SE to the server.
Client segments retransmitted	Number of TCP segments retransmitted by the SE to the client.
Sync cookies sent	Number of synchronized (SYN) cookies sent by the SE. TCP requires unacknowledged data to be retransmitted. The server is supposed to retransmit the SYN.ACK packet before giving up and dropping the connection. When SYN.ACK arrives at the client but the ACK gets lost, there is a disparity about the establishment state between the client and server. Typically, this problem can be solved by the server's retransmission. But in the case of a SYN cookie, there is no state kept on the server and retransmission is impossible.
Sync cookies received	Number of SYN cookies received by the SE. The entire process of establishing the connection is performed by the ACK packet sent by the client, making the connection process independent of the preceding SYN and SYN.ACK packets. This type of connection establishment opens the possibility of ACK flooding, in the hope that the client has the correct value to establish a connection. This method also allows you to bypass firewalls that normally only filter packets with SYN bit set.
Sync cookies failed	Number of SYN cookies rejected by the SE. The SYN cookies feature attempts to protect a socket from a SYN flood attack. This feature is a violation of TCP and conflicts with other areas of TCP such as TCP extensions. It can cause problems for clients and relays. We do not recommend that you use this feature as a tuning mechanism for heavily loaded servers to help with overloaded or misconfigured conditions.
Embryonic connection resets	Number of TCP connections that have been reset before the SE accepted the connection.
Prune message called	Number of calls that the SE makes to the function that tries to reduce the number of received but not acknowledged packets.
Packets pruned from receive queue	Number of packets that the TCP drops from the receive queue (usually because of low memory).

Table 2-60 show statistics tcp Field Descriptions (continued)

Field	Description
Out-of-order-queue pruned	Number of times that the packet was dropped from the out-of-order queue.
Out-of-window Icmp messages	Number of Internet Control Message Protocol (ICMP) packets that were outside the TCP window and dropped.
Lock dropped Icmp messages	Number of ICMP packets that hit a locked (busy) socket and were dropped.
Arp filter	Number of Address Resolution Protocols (ARPs) not sent because they were meant for the SE.
Time-wait sockets	Number of current sockets in the TIME-WAIT state. The TIME-WAIT state removes old duplicates for fast or long connections. The clock-driven ISN selection is unable to prevent the overlap of the old and new sequence spaces. The TIME-WAIT delay allows enough time for all old duplicate segments to die in the Internet before the connection is reopened.
Time-wait sockets recycled	Number of TIME-WAIT sockets that were recycled (the address or port was reused before the waiting period was over). In TCP, the TIME-WAIT state is used as protection against old duplicate segments
Time-wait sockets killed	Number of TIME-WAIT sockets that were terminated to reclaim memory.
PAWS passive	Number of passive connections that were made with Protection Against Wrapped Sequence (PAWS) numbers enabled. PAWS operates within a single TCP connection using a state that is saved in the connection control block.
PAWS active	Number of active connections that were made with PAWS enabled. PAWS uses the same TCP time stamps as the round-trip time measurement mechanism and assumes that every received TCP segment (including the data and ACK segments) contains a time stamp SEG.TSval that has values that are monotone and nondecreasing in time. A segment can be discarded as an old duplicate if it is received with a time stamp SEG.TSval less than some time stamp recently received on this connection.
PAWS established	Number of current connections that were made with PAWS enabled.
Delayed acks sent	Number of delayed ACK counters sent by the SE.
Delayed acks blocked by socket lock	Number of delayed ACK counters that were blocked because the socket was in use.
Delayed acks lost	Number of delayed ACK counters lost during transmission.
Listen queue overflows	Number of times that the three-way TCP handshake was completed, but enough space was not available in the listen queue.

Table 2-60 show statistics tcp Field Descriptions (continued)

Field	Description
Connections dropped by listen queue	Number of TCP connections dropped because of a resource shortage.
TCP packets queued to prequeue	Number of TCP packets queued to the prequeue.
TCP packets directly copied from backlog	Number of TCP packets delivered to the client from the backlog queue. Packets are queued in the backlog when the TCP receive routine runs and notices that the socket was locked.
TCP packets directly copied from prequeue	Number of TCP packets delivered to the client from the prequeue.
TCP prequeue dropped packets	Number of TCP packets dropped from the prequeue. The prequeue is where the TCP receives routine runs. It notes that the current running process as the TCP target process and queues it directly for copy after the TCP software interrupt is completed.
TCP header predicted packets	Number of incoming packets that successfully matched the TCP header prediction.
Packets header predicted and queued to user	Number of TCP packets copied directly to the user space.
TCP pure ack packets	Number of acknowledgment (ACK) packets that contain no data.
TCP header predicted acks	Number of incoming ACKs that successfully matched the TCP header prediction.
TCP Reno recoveries	Number of times that the TCP fast recovery algorithm recovered a packet loss. TCP Reno induces packet losses to estimate the available bandwidth in the network. When there are no packet losses, TCP Reno continues to increase its window size by one during each round trip. When it experiences a packet loss, it reduces its window size to one half of the current window size. This feature is called *additive increase and multiplicative decrease*. TCP Reno, however, does not fairly allocate bandwidth because TCP is not a synchronized rate-based control scheme, which is necessary for the convergence.
TCP SACK recoveries	Number of times that the SE recovered from a SACK packet loss. If the data receiver has received a SACK-permitted option on the SYN for this connection, the data receiver may choose to generate SACK options. If the data receiver generates SACK options under any circumstance, it should generate them under all permitted circumstances. If the data receiver has not received a SACK-permitted option for a given connection, it must not send SACK options on that connection.

Table 2-60 show statistics tcp Field Descriptions (continued)

Field	Description
TCP SACK reneging	Number of times that the SE refused to accept packets that have not been acknowledged to the data sender, even if the data has already been reported in a SACK option. Such discarding of SACK packets is discouraged but may be used if the receiver runs out of buffer space. The data receiver may choose not to keep data that it has reported in a SACK option. Because the data receiver may later discard data reported in a SACK option, the sender must not discard data before it is acknowledged by the Acknowledgment Number field in the TCP header.
TCP FACK reorders	Number of Forward Acknowledgment (FACK) packets that were out of sequence order. The FACK algorithm makes it possible to treat congestion control during recovery in the same manner as during other parts of the TCP state space. The FACK algorithm is based on first principles of congestion control and is designed to be used with the proposed TCP SACK option. By decoupling congestion control from other algorithms, such as data recovery, it attains more precise control over the data flow in the network. FACK takes advantage of the SACK option; it takes into account which segments have been SACKed. It also uses the receipt of a SACK that leaves at least 3*MSS bytes unacknowledged as a trigger for Fast Retransmit.
TCP SACK reorders	Number of Selective Acknowledgment (SACK) packets that were out of sequence order.
TCP Reno reorders	Number of TCP Renos that were out of sequence order.
TCP TimeStamp reorders	Number of segments received with out-of-order time stamps.
TCP full undos	Number of times that the congestion window (cwnd) was fully recovered.
TCP partial undos	Number of times that the congestion window (cwnd) was partially recovered.
TCP DSACK undos	Number of times that the Duplicate Selective Acknowledgment (D-SACK) packets were recovered.
TCP loss undos	Number of times that the congestion window (cwnd) recovered from a packet loss.
TCP losses	Number of times that data was lost and the size of the congestion window (cwnd) decreased.
TCP lost retransmit	Number of times that a retransmitted packet was lost.

Table 2-60 show statistics tcp Field Descriptions (continued)

Field	Description
TCP Reno failures	Number of times that the congestion window (cwnd) failed because the TCP fast recovery algorithm failed to recover from a packet loss. The congestion avoidance mechanism, which is adopted by TCP Reno, causes the window size to vary. This situation causes a change in the round-trip delay of the packets, larger delay jitter, and an inefficient use of the available bandwidth because of many retransmissions of the same packets after the packet drops occur. The rate at which each connection updates its window size depends on the round-trip delay of the connection. The connections with shorter delays can update their window sizes faster than other connections with longer delays.
TCP SACK failures	Number of times that the congestion window (cwnd) shrunk because the SE failed to recover from a SACK packet loss. The selective acknowledgment extension uses two TCP options. The first is an enabling option, SACK-permitted, which may be sent in a SYN segment to indicate that the SACK option can be used once the connection is established. The other is the SACK option, which may be sent over an established connection once permission has been given by the SACK-permitted option.
TCP loss failures	Number of times that the TCP timeout occurred and data recovery failed.
TCP fast retransmissions	Number of TCP fast retransmission counters. TCP may generate an immediate acknowledgment (a duplicate ACK) when an out-of-order segment is received. The duplicate ACK lets the other end know that a segment was received out of order and tells it what sequence number is expected. Because TCP does not know whether a duplicate ACK is caused by a lost segment or just a reordering of segments, it waits for a small number of duplicate ACKs to be received. If there is just a reordering of the segments, there is only one or two duplicate ACKs before the reordered segment is processed, which then generates a new ACK. If three or more duplicate ACKs are received in a row, it is a strong indication that a segment has been lost. TCP then retransmits what appears to be the missing segment without waiting for a retransmission timer to expire.

Table 2-60 show statistics tcp Field Descriptions (continued)

Field	Description
TCP forward retransmissions	Number of TCP forward retransmission counters. This field applies only to SACK-negotiated connections; this field is the counter for FACK segments. The value of this field is for segments that were retransmitted even though there is no indication that they were actually lost. Retransmission is stopped when either one of the following occurs: • Maximum time to wait for a remote response is reached. This timeout occurs when the total time of all retransmission intervals exceeds the maximum time to wait for a remote response. • Number of retransmissions configured in maximum retransmissions per packet is reached.
TCP slowstart retransmissions	Number of TCP slow-start retransmission counters. The slow-start algorithm begins by sending packets at a rate that is determined by the congestion window. The algorithm continues to increase the sending rate until it reaches the limit set by the slow-start threshold (ssthresh) variable. (Initially, the value of the ssthresh variable is adjusted to the receiver's maximum window size [RMSS]. However, when congestion occurs, the ssthresh variable is set to half the current value of the cwnd variable, marking the point of the onset of network congestion for future reference.)
TCP Timeouts	Number of times that a TCP timeout occurred.
TCP Reno recovery fail	Number of times that the TCP fast recovery algorithm failed to recover from a packet loss. In TCP Reno, the maximum number of recoverable packet losses in a congestion window without timeout is limited to one or two packets. No more than six losses can be recovered with a maximum window size of 128 packets. This failure of recovery is because TCP Reno cuts the congestion window by half for each recovered loss.
TCP Sack recovery fail	Number of times that the SE failed to recover from a SACK packet loss. When receiving an ACK containing a SACK option, the data sender should record the selective acknowledgment for future reference. The data sender is assumed to have a retransmission queue that contains the segments that have been sent but not yet acknowledged in sequence number order. If the data sender performs repacketization before retransmission, the block boundaries in a SACK option that it receives may not fall within the boundaries of segments in the retransmission queue.
TCP scheduler failed	Number of times that the TCP scheduler failed.
TCP receiver collapsed	Number of times that the data in an out-of-order queue collapsed.

Table 2-60 show statistics tcp Field Descriptions (continued)

Field	Description
TCP DSACK old packets sent	Number of D-SACKs sent by the SE. The use of D-SACK does not require a separate negotiation between a TCP sender and receiver that have already negotiated SACK. The absence of a separate negotiation for D-SACK means that the TCP receiver could send D-SACK blocks when the TCP sender does not understand this extension to SACK. In this case, the TCP sender discards any D-SACK blocks and processes the other SACK blocks in the SACK option field as it normally would.
TCP DSACK out-of-order packets sent	Number of out-of-order D-SACK packets sent by the SE. A D-SACK block is used only to report a duplicate contiguous sequence of data received by the receiver in the most recent packet. Each duplicate contiguous sequence of data received is reported in at most one D-SACK block. (The receiver sends two identical D-SACK blocks in subsequent packets only if the receiver receives two duplicate segments.) If the D-SACK block reports a duplicate contiguous sequence from a (possibly larger) block of data in the receiver's data queue above the cumulative acknowledgement, then the second SACK block in that SACK option should specify that (possibly larger) block of data.
TCP DSACK packets received	Number of D-SACK packets received by the SE. TCP senders receiving D-SACK blocks should be aware that a segment reported as a duplicate segment could possibly have been from a prior cycle through the sequence number space. This awareness of the TCP senders is independent of the use of PAWS by the TCP data receiver.
TCP DSACK out-of-order packets received	Number of out-of-order D-SACK packets received by the SE. Following a lost data packet, the receiver receives an out-of-order data segment, which triggers the SACK option as specified in RFC 2018. Because of several lost ACK packets, the sender then retransmits a data packet. The receiver receives the duplicate packet and reports it in the first D-SACK block.
TCP connections abort on sync	Number of times that a valid SYN segment was sent in the TCP window and the connection was reset.
TCP connections abort on data	Number of times that the connection closed after reading the data.
TCP connections abort on close	Number of times that the connection aborted with pending data.
TCP connections abort on memory	Number of times that memory was not available for graceful closing of the connection resulting in the connection being aborted immediately.
TCP connections abort on timeout	Number of times that the connection timed out.
TCP connections abort on linger	Number of times that the linger timeout expired resulting in the data being discarded and closing of the connection.

Table 2-60 show statistics tcp Field Descriptions (continued)

Field	Description
TCP connections abort failed	Number of times that the TCP connection ran out of memory, transmits failed, or peer TCP Reset (RST) could not be sent.
TCP memory pressures	Number of times that the TCP subsystem encounters memory constraints.

Related Commands

Command	Description
clear statistics	Clears the statistics settings.

show statistics transaction-logs

To display SE transaction log export statistics, use the **show statistics transaction-logs** command in EXEC configuration mode.

show statistics transaction-logs

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

To display the transaction log export statistics, you must first configure the File Transfer Protocol (FTP) server.

Table 2-61 describes the fields shown in the **show statistics transaction-logs** display.

Table 2-61 show statistics transaction-logs Field Descriptions

Field	Description
Initial Attempts	Initial attempts made to contact the external server at the configured export intervals.
Initial Successes	Number of times that an initial attempt made to contact the external server succeeded.
Initial Open Failures	Number of times that the SE failed to open a connection to the FTP export server.
Initial Put Failures	Number of times that the SE failed to transfer a file to the File Transfer Protocol (FTP) export server.
Retry Attempts	Number of retries made to contact the external server at the configured export intervals.
Retry Successes	Number of times that a retry made to contact the external server succeeded.
Retry Open Failures	Number of times that the SE failed to open a connection to the FTP export server on a retry.
Retry Put Failures	Number of times that the SE failed to transfer a file to the FTP export server on a retry.
Authentication Failures	Number of times that the SE failed to authenticate with the FTP export server. This situation might occur if the SE is misconfigured with the wrong password for the FTP server or the password on the FTP server has been changed since the SE was configured.
Invalid Server Directory Failures	Number of times the SE failed to direct traffic to the correct server directory.

Related Commands

Command	Description
clear transaction-log	Clears the working transaction logs settings.
show transaction-logging	Displays the transaction log configuration settings and a list of archived transaction log files.
transaction-log force	Forces the archive or export of the transaction log.

show statistics udp

To display SE User Datagram Protocol (UDP) statistics, use the **show statistics udp** command in EXEC configuration mode.

show statistics udp

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-62 describes the fields shown in the **show statistics udp** display.

Table 2-62 show statistics udp Field Descriptions

Field	Description
Packets received	Total number of UDP packets received.
Packets to unknown port received	Number of packets to unknown ports received.
Packet receive error	Number of packet receive errors.
Packet sent	Number of UDP packets sent.

show statistics vos

To display Videoscape Distribution Suite Origin Server (VDS-OS) statistics, use the **show statistics vos** command in EXEC configuration mode.

show statistics vos {**errors** | **rm-interface** | **vosm-interface** | **we-interface**}

Syntax Description

errors	Displays error statistics.
rm-interface	Displays Recording Manager interface statistics.
vosm-interface	Displays VOSM interface statistics.
we-interface	Displays Web Engine Interface Statistics

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-63 describes the fields shown in the **show statistics vos** display.

Table 2-63 show statistics vos Field Descriptions

Field	Description
VDS-OS Statistics	
Origin Services Created	Total number of Origin Services created successfully on the SE.
Origin Services Deleted	Total number of Origin Services deleted successfully on the SE.
Channels Created	Total number of channels created successfully on the SE.
Channels Deleted	Total number of channels deleted successfully on the SE.
Live Publish Resources Configured	Total number of Live Publish Resource configurations received from the VOSM.
Live Publish Resources Created	Total number of Live Publish Resources created successfully on the SE. Starting a publish resource administratively after it is stopped counts as an additional create.
Live Publish Resources Deleted	Total number of Live Publish Resources deleted successfully by the SE. Stopping a publish resource administratively counts as an additional delete.
Scheduled Publish Resources Configured	Total number of Live-to-VOD Publish Resource configurations received from the VOSM/Recorder Manager.
Scheduled Publish Resources Created	Total number of Live-to-VOD Publish Resources created successfully on the SE.

Table 2-63 show statistics vos Field Descriptions (continued)

Field	Description
Scheduled Publish Resources Deleted	Total number of Live-to-VOD Publish Resources deleted successfully by the SE. Although these Publish Resources are deleted from the SE on completion, the recorded content continues to be stored on the Network-Attached Storage (NAS).
Current Active Live Publish Resources	The number of Live Publish Resources for which content is currently being ingested.
Current Active Scheduled Publish Resources	The number of Live-to-VOD Publish Resources for which content is currently being ingested.
Error Statistics	
Channel Failures	Total number of channel failures encountered.
Live Publish Resource Failures	Total number of Live Publish Resources that have failed completely (partial failures such as few streams failing are not accounted for).
Scheduled Publish Resource Failures	Total number of Live-to-VOD Publish Resources that have failed completely.
Capture Resource Failures	Total number of failed/partially failed Capture Resources.
Capture Stream Failures	Total number of failed Capture Streams/Profiles.
Publish Stream Failures	Total number of failed Publish Streams/Profiles.
Parsing/Validation Failures	Total number of failures in parsing or validating Channel/Schedule Configuration received from the VOSM.
VOSM Communication Failures	Total number of failures in sending Notification messages to VOSM.
RM Communication Statistics	
Start Recording Requests	The number of create recording event messages received from recorder manager.
Modify Recording Requests	The number of modify recording event messages received from recorder manager.
Recording Status Requests	The number of get recording event status messages received from recorder manager.
Cancel Recording Requests	The number of cancel recording event messages received from recorder manager.
Get Recording List Count Requests	The number of get recording event count messages received from recorder manager.
Get Recording List Requests	The number of get recording event list messages received from recorder manager.
Notification To RM	The number of notification messages sent by VDS-OS to recorder manager.
RM Communication Error Statistics	
RM Communication Failures	The total number of failures when communicating to the recorder manager.
HTTP Bad Request	The total number of HTTP 400 responses sent to the recorder manager.
HTTP Not Found	The total number of HTTP 404 responses sent to the recorder manager.

Table 2-63 show statistics vos Field Descriptions (continued)

Field	Description
Internal server Error	The total number of HTTP 500 responses sent to the recorder manager.
Communication Failures	Total number of failures in sending Notification messages to RM
VOSM Communication Statistics	
Origin Service Creates/Updates	Total number of Origin Service Create/Update notifications received from VOSM.
Origin Service Deletes	Total number of Origin Service Delete notifications received from VOSM.
Channel Config Creates	Total number of New Channel Configuration notifications received.
Channel Config Updates	Total number of Updates to existing channels received.
Channel Config Deletes	Total number of Channel Config Delete notifications received.
Schedule Config Creates	Total number of New Schedule Config notification received.
Schedule Config Updates	Total number of Updates to existing Schedule Config received.
Schedules Config Deletes	Total number of Schedule Config Delete notifications received.
Start Channel Commands	Total number of Start Channel Control Commands received from VOSM.
Stop Channel Commands	Total number of Stop Channel Control Commands received from VOSM.
Start Capture Resource Commands	Total number of Start Capture Resource Control Command received from VOSM.
Stop Capture Resource Commands	Total number of Stop Capture Resource Control Command received from VOSM.
Start Publish Resource Commands	Total number of Start Publish Resource Control Command received from VOSM.
Stop Publish Resource Commands	Total number of Stop Publish Resource Control Command received from VOSM.
Resource Notifications	Total number of Channel/CaptureResource/PublishResource status notification messages sent to VOSM.
Resource Status Queries	Total number of Global/Channel/CaptureResource/Publish Resource status notification requests received from VOSM.
VOSM Heartbeats	Total number of Heartbeats received from CMS agent.
VOSM Communication Error Statistics	Total number of failures in honoring the respective config notification/control commands received from the VOSM.
Channel Parsing/Validation Failures	Total number of parsing/validation errors with the Channel/Schedule config Extensible Markup Language (XML) files received from VOSM.
Origin Service Create Failures	Total number of failed Origin Service Creates.
Origin Service Delete Failures	Total number of failed Origin Service Deletes.
Channel Config Create Failures	Total number of failed Channel Config Creates.
Channel Config Update Failures	Total number of failed Channel Config Updates.

Table 2-63 show statistics vos Field Descriptions (continued)

Field	Description
Channel Config Delete Failures	Total number of failed Channel Config Deletes.
Schedule Config Create Failures	Total number of failed Scheduled ConfigCreates.
Schedule Config Update Failures	Total number of failed Schedule Config Updates.
Schedule Config Delete Failures	Total number of failed Schedule Config Deletes.
Start Channel Command Failures	Total number of failed Start Channel Command.
Stop Channel Command Failures	Total number of failed Stop Channel Commands.
Start Capture Resource Failures	Total number of failed Start Capture Resources.
Stop Capture Resource Failures	Total number of failed Stop Capture Resources.
Start Publish Resource Failures	Total number of failed Start Publish Resources.
Stop Publish Resource Failures	Total number of failed Stop Publish Resources.
Resource Notification Failures	Total number of failures in sending Channel/CaptureResource/PublishResource status notification messages to the VOSM.
Resource Status Query Failures	Total number of failures in responding to Global/Channel/CaptureResource/PublishResource status notification requests received from VOSM.
WE Communication statistics	These are cumulative statistics that account for the interaction between Capture Controller and Web Engine.
Create Channel	Total number of Create Channel messages sent to the Web Engine. This message is sent each time a channel is administratively started.
Create Capture Resource	Total number of Create Capture Resource messages sent to the Web Engine. This message configures the ingest profiles to expect from the Upstream Encapsulators and is sent to the Web Engine each time the Capture resource is started (either on channel restart or capture resource restart).
Create Publish Resource	Total number of Create Publish Resource messages sent to the Web Engine. This message configures the publish points and the required profiles to be stored on the NAS. It is sent to the Web Engine each time the Publish Resource is started (at the configured start time) or when a stream recovers.
Update Publish Resource	Total number of Update Publish Resource messages sent to the Web Engine. This message updates the stop time of a currently active Publish Resource.

Table 2-63 show statistics vos Field Descriptions (continued)

Field	Description
Stop Channel	Total number of Stop Channel messages sent to the Web Engine. This message is sent when the channel is administratively stopped/deleted by the operator.
Stop Capture Resource	Total number of Stop Capture Resource messages sent to the Web Engine. This message is sent when either the capture resource or the channel is stopped or deleted.
Stop Publish Resource	Total number of Stop Publish Resource messages sent to the Web Engine. This message is sent to stop active publish resources when the corresponding Capture Resource or Publish Resource itself is stopped, or when the channel is deleted/stopped.
Delete Publish Resource	Total number of Delete Publish Resource messages sent to the Web Engine. This message is sent to delete the asset stored on the NAS when the explicitly requested by the RM or to delete live assets when channel is being deleted.
Publish Resource Status Notify	Total number of Publish Resource Failure/Recovery notifications sent by the Web Engine.
Capture Resource Status Notify	Total number of Capture Resource Failure/Recover notifications sent by the Web Engine. Currently a separate message is sent for each Stream Failure/Recovery.
Web Engine Registration	Total number of registrations sent by the Web Engine to the Capture Controller every time the Web Engine restarts.
WE Communication Error Statistics	Total number of failures in sending the respective messages to Web Engine.
WE Communication Failures	Total number of failures in sending a message to Web Engine.
Create Channel Failures	Total number of failed Channel Creates.
Create Capture Resource Failures	Total number of failed Capture Resource Creates.
Create Publish Resource Failures	Total number of failed Publish Resource Creates.
Update Publish Resource Failures	Total number of failed Publish Resource Updates.
Stop Channel Failures	Total number of failed Stop Channels.
Stop Capture Resource Failures	Total number of failed Capture Resource Stops.
Stop Publish Resource Failures	Total number of failed Publish Resource Stops.
Delete Publish Resource Failures	Total number of failed Publish Resource Deletes.

Table 2-63 show statistics vos Field Descriptions (continued)

Field	Description
Publish Resource Status Notify Failures	Total number of failures in processing the Publish Resource Status Notification from Web Engine [Publish Resource not found, Parsing errors).
Capture Resource Status Notify Failures	Total number of failures in processing the Capture Resource Status Notification from Web Engine (Capture Resource not found, Parsing errors).

Examples

The follow example shows how to display the VDS-OS statistics:

```
ServiceEngine# show statistics vos

VDS-OS Statistics
----------------------------------

Origin Services Created                 :                       0
Origin Services Deleted                 :                       0
Channels Created                        :                       0
Channels Deleted                        :                       0
Live Publish Resources Configured       :                       0
Live Publish Resources Created          :                       0
Live Publish Resources Deleted          :                       0
Scheduled Publish Resources Configured  :                       0
Scheduled Publish Resources Created     :                       0
Scheduled Publish Resources Deleted     :                       0
Current Active Live Publish Resources   :                       0
Current Active Scheduled Publish Resources:                     0

Error  Statistics
----------------------------------

Channel Failures                        :                       0
Live Publish Resource Failures          :                       0
Scheduled Publish Resource Failures     :                       0
Capture Resource Failures               :                       0
Capture Stream Failures                 :                       0
Publish Stream Failures                 :                       0
Parsing/Validation Failures             :                       0
VOSM Communication Failures             :                       0
RM Communication Failures               :                       0
```

The follow example shows how to display the VDS-OS error statistics:

```
ServiceEngine# show statistics vos errors
```

The follow example shows how to display the Recording Manager interface statistics:

```
ServiceEngine# show statistics vos rm-interface

RM Communication Statistics
----------------------------------

Start Recording Requests                :                       0
Modify Recording Requests               :                       0
Recording Status Requests               :                       0
Delete Recording Requests               :                       0
Cancel Recording Requests               :                       0
Get Recording List Count Requests       :                       0
```

```
Get Recording List Requests             :                        0
Notification To RM                      :                        0

Error  Statistics
-----------------------------------

RM Communication Failures               :                        0
HTTP Bad Request                        :                        0
HTTP Not Found                          :                        0
Internal server Error                   :                        0
```

The follow example shows how to display the VOSM interface statistics:

```
ServiceEngine# show statistics vos vosm-interface

VOSM Communication Statistics
-----------------------------------

Origin Service Creates/Updates          :                        0
Origin Service Deletes                  :                        0
Channel Config Creates                  :                        0
Channel Config Updates                  :                        0
Channel Config Deletes                  :                        0
Schedule Config Creates                 :                        0
Schedule Config Updates                 :                        0
Schedules Config Deletes                :                        0
Start Channel Commands                  :                        0
Stop Channel Commands                   :                        0
Start Capture Resource Commands         :                        0
Stop Capture Resource Commands          :                        0
Start Publish Resource Commands         :                        0
Stop Publish Resource Commands          :                        0
Resource Notifications                  :                        0
Resource Status Queries                 :                        0
VOSM Heartbeats                         :                      579

Error  Statistics
-----------------------------------

Channel Parsing/Validation Failures     :                        0
Origin Service Create Failures          :                        0
Origin Service Delete Failures          :                        0
Channel Config Create Failures          :                        0
Channel Config Update Failures          :                        0
Channel Config Delete Failures          :                        0
Schedule Config Create Failures         :                        0
Schedule Config Update Failures         :                        0
Schedule Config Delete Failures         :                        0
Start Channel Command Failures          :                        0
Stop Channel Command Failures           :                        0
Start Capture Resource Failures         :                        0
Stop Capture Resource Failures          :                        0
Start Publish Resource Failures         :                        0
Stop Publish Resource Failures          :                        0
Resource Notification Failures          :                        0
Resource Status Query Failures          :                        0
```

The follow example shows how to display the Web Engine statistics:

```
ServiceEngine# show statistics vos we-interface

WE Communication statistics
-----------------------------------
```

```
Create Channel                          :                       0
Create Capture Resource                 :                       0
Create Publish Resource                 :                       0
Update Publish Resource                 :                       0
Stop Channel                            :                       0
Stop Capture Resource                   :                       0
Stop Publish Resource                   :                       0
Delete Publish Resource                 :                       0
Publish Resource Status Notify          :                       0
Capture Resource Status Notify          :                       0
Web Engine Registration                 :                       0

Error  Statistics
-----------------------------------

WE Communication Failures               :                       0
Create Channel Failures                 :                       0
Create Capture Resource Failures        :                       0
Create Publish Resource Failures        :                       0
Update Publish Resource Failures        :                       0
Stop Channel Failures                   :                       0
Stop Capture Resource Failures          :                       0
Stop Publish Resource Failures          :                       0
Delete Publish Resource Failures        :                       0
Publish Resource Status Notify Failures :                       0
Capture Resource Status Notify Failures :                       0
```

Related Commands

Command	Description
show vos	Displays VDS-OS services.

show statistics web-engine

To display the Web Engine statistics, use the **show statistics web-engine** command in EXEC configuration mode.

show statistics web-engine
[
abr
{
dash-media-app
[
detail |
fragment-file |
manifest-file |
representation-index-file |
server-manifest-file | **summary**
] |
hls-media-app
[
detail |
fragment-file |
manifest-file |
meta-file |
session | **summary**
] |
smoothhd-media-app
[
detail |
fragment-file |
manifest-file |
meta-file |
session |
summary
] |
zeri-media-app
[
detail |
fragment-file |
manifest-file |
meta-file |
session |
summary
]
} |
detail |
error summary |
key-client |
performance |
usage
]

Syntax Description

abr	(Optional) Adaptive Bit-Rate streaming statistics.
dash-media-app	(Optional) Displays DASH-Media-App statistics.
detail	(Optional) Displays DASH-Media-App Detail statistics.
fragment-file	(Optional) Displays DASH-Media-App Fragment-File statistics.
manifest-file	(Optional) Displays DASH-Media-App Manifest-File statistics.
representative-index-file	(Optional) Displays DASH-Media-App Representative-Index-File statistics.
service-manifest-file	(Optional) Displays DASH-Media-App-Server-Manifest-File statistics.
summary	(Optional) Displays DASH-Media-App summary.
hls-media-app	(Optional) Displays HLS-Media-App statistics.
detail	(Optional) Displays HLS-Media-App Detail statistics.
fragment-file	(Optional) Displays HLS-Media-App Fragment-File statistics.
manifest-file	(Optional) Displays HLS-Media-App Manifest-File statistics.
meta-file	(Optional) Displays HLS-Media-App Meta-File statistics.
session	(Optional) Displays HLS-Media-App Session statistics.
summary	(Optional) Displays HLS-Media-App summary.
smoothhd-media-app	(Optional) Displays SmoothHD-Media-App statistics.
detail	(Optional) Displays SmoothHD-Media-App Detail statistics.
fragment-file	(Optional) Displays SmoothHD-Media-App Fragment-File statistics.
manifest-file	(Optional) Displays SmoothHD-Media-App Manifest-File statistics.
meta-file	(Optional) Displays SmoothHD-Media-App Meta-File statistics.
session	(Optional) Displays SmoothHD-Media-App Session statistics.
summary	(Optional) Displays SmoothHD-Media-App summary.
zeri-media-app	(Optional) Displays Zeri-Media-App statistics.
detail	(Optional) Displays Zeri-Media-App Detail statistics.
fragment-file	(Optional) Displays Zeri-Media-App Fragment-File statistics.
manifest-file	(Optional) Displays Zeri-Media-App Manifest-File statistics.
meta-file	(Optional) Displays Zeri-Media-App Meta-File statistics.
session	(Optional) Displays Zeri-Media-App Session statistics. **Note** The **zeri-media-app session** option is not supported in VDS-OS 2.0.
summary	(Optional) Displays Zeri-Media-App summary.
detail	(Optional) Displays detail statistics.
error	(Optional) Displays error statistics.
summary	(Optional) Displays statistics based on 4xx/5xx response codes.
key-client	(Optional) Displays key client statistics.
performance	(Optional) Displays performance statistics.
usage	(Optional) Displays usage statistics.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The Web Engine must be running to see the statistics. The Web Engine is running by default.

Note A client request to an edge SE triggers a liveness query to the upstream SEs and Content Acquirer. Even after the client connection is closed, the liveness query continues for up to ten minutes. This is to keep the SEs ready with liveness states for subsequent client requests.

The **show statistics web-engine detail** command output also displays Web Engine memory usage. This can increase to greater than 2 GB and can stay above 2 GB even after traffic subsides. This is expected behavior and does not indicate a memory leak.

Table 2-64 describes the fields shown in the **show statistics web-engine** display.

Table 2-64 show statistics web-engine Field Descriptions

Field	Description
HTTP Request Info Statistics	
Num Lookups	Number of Content Abstraction Layer (CAL) lookups done.
Preposition Hit	Number of preposition hit requests. This statistic is only incremented at the end of the session life.
External Hit	Displays Network-Attached Storage (NAS) Origin Hit count.
Cache Hit	Number of requests that resulted in a cache hit. This statistic is only incremented at the end of the session life.
Cache Miss	Number of requests that resulted in a cache miss (the web object was not available in the cache).
Partial Cache Hit	Number of cacheable requests that were partial cache hits. This statistic is only incremented at the end of the session life.
Cache Bypass	Whenever the Web Engine receives either a large file range request or a request type that it cannot cache. This statistics counter increases and the request file is not cached. This statistic is only incremented at the end of the session life.
Live Miss	Session miss for MP3 Live streaming over HTTP.
Live Hit	Session hit for MP3 Live streaming over HTTP.
ASX Meta Response	Incremented when a Windows Media Live Request(.asx) request is processed by the Web Engine.
HTTP Request Type Statistics	
Get Requests	Total Get requests.
Post Requests	Total Post requests.
Head Requests	Total Head requests.

Table 2-64 show statistics web-engine Field Descriptions (continued)

Field	Description
Range Requests Received	Range requests from clients.
Range Requests Sent	Requests sent to OS liveness query.
Revalidation Requests Received	Revalidation requests from clients. This counter is incremented only when an If-Modified-since (IMS) request is received by the Streamer.
Revalidation Requests Sent	Revalidation requests to OS liveness query.
Liveness Query	Liveness query received from the downstream SE. Liveness queries are sent even when there are no client requests and liveness updates are sent every ten minutes, so it is not mandatory to have client request in order to generate a liveness query.
Local Requests	Requests from other Protocol Engines.
Total Outgoing Requests	Total number of unique request that the Web Engine sent to the upstream.
Origin Services Redirected Requests	Cumulative sum of requests coming to all delivery services on the SE for which this feature is enabled. This number is cleared when the Web Engine is restarted or the **clear statistics all** command is executed.
HTTP Authorization Statistics	
Authorization Allow	Number of authorization requests being allowed.
Authorization No Cache	Number of authorization requests being applied with the No-cache rule.
Authorization Force Revalidate	Number of authorization requests being applied with the Force revalidate rule.
Authorization Deny	Number of authorization requests being denied.
Authorization Rewrite	Number of authorization requests being applied with the rewrite rule.
Authorization GenerateSign	Number of authorization requests being applied with the generate sign rule.
Authorization Redirect	Number of authorization requests being redirected.
Authorization Resolve	Number of authorization requests being applied with the URL-Resolve rule.
HTTP Error Statistics	
Client Errors	Number of 4xx errors.
Server Errors	Number of 5xx errors.
Bad Requests	Number of HTTP request corruptions.
Error Response Hit	Number of error response cache hits.
Error Response Miss	Number of error response cache misses. With error response caching enabled, the error responses like 404 and 503 could be cached.
HTTP Performance Statistics	

Table 2-64 show statistics web-engine Field Descriptions (continued)

Field	Description
Total Bytes In	Total bytes in. This statistic is only incremented at the end of the session life.
Total Bytes Out	Total bytes out. This statistic is only incremented at the end of the session life.
Total Requests	Total requests since last Web Engine statistics cleared time.
Average Request Per Second	Average requests per second. **Note** To get an accurate request per second reading in a given time period, clear the Web Engine statistics first and then generate the **shows statistics web-engine** command.
Average Bytes Per Second	Average number of bytes per second since the last Web Engine statistics were cleared.
Web Engine Detail Statistics	
Active HTTPSession	HTTPSession is unique to the end user connection. This value counts the HTTP request targeted to port 80, regardless of which Protocol Engine handles the request. The sample rate and Real-Time value are calculated at the time the command is executed.
Active DataSource	Sources used to fetch the data. Disk for cache hit; OS for cache miss.
Active HTTPDataFeed	Active connections to the Origin Services or upstream SE's to fetch Data.
Active HTTPData SourceFinder	The number of active DataSourceFinder present. DataSourceFinder is responsible for creating the datasource.
Active HTTPTransaction	On a given session, this is the number of active pipeline transactions the Web Engine is currently processing.
Pending HTTPTransaction	On a given session, this is the number of pending pipeline transactions the Web Engine has yet to process.
Active ServerXact	HTTP Request currently under process.
Total HTTPConnection	Total outgoing HTTP connection to upstream.
Active HTTPConnection	HTTP connection currently serving request.
Idle Proxy HTTPConnection	Intra-SE connection in the idle queue.
Idle Origin HTTPConnection	Non-Intra-SE/Origin Services connection in the idle queue.
Memory Hit	Number of requested files available in /tmpfs. This statistic is only incremented at the end of the session life.
Cut-Thru Counter	Number of cached files deleted without moving to disk.
Memory Usage	Memory usage of the Web Engine process.

Table 2-64 show statistics web-engine Field Descriptions (continued)

Field	Description
Web Engine Trickle Status	This flag is set when the Web Engine has exceeded thresholds but cannot restart because of outstanding sessions. When the transactions on HTTPSessions complete, it looks at this trickle flag and terminates the connection instead of processing the next request on the connection. This flag is reset to 0 when memory usage is low because the number of sessions has decreased. If the number of sessions goes to 0 and memory usage is still high, the Trickle flag is set and the Web Engine restarts.
Outstanding Content Create Requests	Allocates a disk and a file path for a given URL. The protocol engine uses this location to store the downloaded content. The number of outstanding creates reflect the number of such requests to the CAL module that have been submitted but were not completed.
Outstanding Content Lookup Requests	Translates the URL from an end client into a disk path in the case of a cache hit (based on a previous create). In the case of cache miss, it would give the route from where the content can be found. The counter number of outstanding lookups reflects the number of pending requests.
Outstanding Content Delete Requests	Deletes a file created by CAL. The number of outstanding deletes reflects the number of pending delete requests.
Outstanding Content Update Requests	Updates the Content metadata CAL. The number of outstanding updates reflect the number of pending update requests submitted to CAL.
Outstanding Content Popularity Update Requests	Updates the Content Popularity metadata CAL. The number of outstanding updates reflect the number of pending update requests submitted to CAL.
Media Manifest File Statistics	
Dynamic Ingest Mem Hit	Number of cache hits on client manifest.
Dynamic Ingest Mem Miss	Number of cache misses on client manifest.
Media Fragment File Statistics	
Dynamic Ingest Mem Hit	Number of cache hits on .ts file.
Dynamic Ingest Mem Miss	Number of cache misses on .ts file.
Media Server Manifest File Statistics	
Dynamic Ingest Mem Hit	Number of cache hits on server manifest.
Dynamic Ingest Mem Miss	Number of cache misses on server manifest.
Media Representation Index File Statistics	
Dynamic Ingest Mem Hit	Number of cache hits on representation file.
Dynamic Ingest Mem Miss	Number of cache misses on representation file.
Media Error Statistics	
Dynamic Ingest cMPD Parsing Error	Number of errors when parsing client manifest file.

Table 2-64 show statistics web-engine Field Descriptions (continued)

Field	Description
Dynamic Ingest sMPD Download Error	Number of errors when downloading server manifest.
Dynamic Ingest sMPD Parsing Error	Number of errors when parsing server manifest.
Dynamic Ingest Fragment Download Error	Number of errors when downloading .ts file.
Dynamic Ingest RepresentationIndex Parsing Error	Number of errors when parsing representation index file.
Dynamic Ingest RepresentationIndex Download Error	Number of errors when downloading representation index file.
Media Detail Statistics	
Dynamic Ingest InProgress Active Assets	Number of in-progress requests on an active asset.
Dynamic Ingest InProgress Request	Total number of in-progress requests.
Dynamic Ingest Complete Request	Total number of completed requests.

Note The "Total Bytes Out" statistic counts the header length but the "Total Bytes In" statistic does not.

Examples

The following example shows how to display the detailed Web Engine statistics:

```
ServiceEngine# show statistics web-engine detail

HTTP Request Info Statistics
----------------------
Num Lookups                   :                 4212308
Preposition Hit               :                       0
External Hit                  :                       0
Cache Hit                     :                   30109
Cache Miss                    :                 4043651
Partial Cache Hit             :                       0
Cache Bypass                  :                       0
Live Miss                     :                       0
Live Hit                      :                       0
ASX Meta Response             :                       0

HTTP Request Type Statistics
----------------------
Get Requests                  :                 4215164
Post Requests                 :                       0
Head Requests                 :                       0
Range Requests Received       :                      10
Range Requests Sent           :                       0
Revalidation Requests Received :                   26921
Revalidation Requests Sent    :                 1003660
Liveness Query                :                    6832
Local Requests                :                       0
Play Live Requests            :                       0
Total Outgoing Requests       :                 4073031

HTTP Authorization Statistics
----------------------
Authorization Allow           :                 4212638
```

```
Authorization No Cache         :                          0
Authorization Force Revalidate :                          0
Authorization Deny             :                          0
Authorization Rewrite          :                          0
Authorization GenerateSign     :                          0
Authorization Redirect         :                          0
Authorization Resolve          :                          0

HTTP Error Statistics
---------------------
Client Errors                  :                          0
Server Errors                  :                     877658
Bad Requests                   :                          0
Error Response Miss            :                          0
Error Response Hit             :                          0

HTTP Performance Statistics
---------------------
Total Bytes In                 :              621029676477
Total Bytes Out                :              594801670055
Total Requests                 :                   4215255
Average Requests Per Second    :                     60.61
Average Bytes Per Second       :                8552759.45

Web Engine Detail Statistics
---------------------
Active HTTPSession             :                         29
Active DataSource              :                        161
Active HTTPDataFeed            :                          0
Active HTTPDataSourceFinder    :                          0
Active HTTPTransaction         :                          1
Pending HTTPTransaction        :                          0
Active ServerXact              :                          0
Total HTTPConnection           :                         12
Active HTTPConnection          :                          0
Idle Proxy HTTPConnection      :                          0
Idle Origin HTTPConnection     :                         12
Memory Hit                     :                        377
Cut-Thru Counter               :                    7390705
Memory Usage                   :                 2297475072
Web Engine Trickle Status      :                          0
Outstanding Content Create Requests:                      0
Outstanding Content Lookup Requests:                      0
Outstanding Content Delete Requests:                      0
Outstanding Content Update Requests:                      0
Outstanding Content Popularity Update Requests:                    0
Statistics was last cleared on Wednesday, 24-Aug-2011 22:18:08 PDT.
ServiceEngine#
```

The following example shows how to display the statistics for the DASH-Media-App:

```
ServiceEngine# show statistics web-engine abr hls-media-app

Media Manifest File Statistics
----------------------
Dynamic Ingest Mem Hit                          :                  0
Dynamic Ingest Cache Miss                       :                  0

Media Fragment File Statistics
----------------------
Dynamic Ingest Mem Hit                          :                  0
Dynamic Ingest Cache Miss                       :                  0

Media Server Manifest File Statistics
```

```
-----------------------
Dynamic Ingest Mem Hit                                :                0
Dynamic Ingest Cache Miss                             :                0

Media Representation Index File Statistics
-----------------------
Dynamic Ingest Mem Hit                                :                0
Dynamic Ingest Cache Miss                             :                0

Media Error Statistics
----------------------
Dynamic Ingest cMPD Parsing Error                     :                0
Dynamic Ingest sMPD Download Error                    :                0
Dynamic Ingest sMPD Parsing Error                     :                0
Dynamic Ingest Fragment Download Error                :                0
Dynamic Ingest RepresentationIndex Parsing Error      :                0
Dynamic Ingest RepresentationIndex Download Error     :                0

Media Detail Statistics
----------------------
Dynamic Ingest InProgress Active Assets               :                0
Dynamic Ingest InProgress Request                     :                0
Dynamic Ingest Complete Request                       :                0
```

The following example shows how to display the statistics for the HLS-Media-App:

```
ServiceEngine# show statistics web-engine abr hls-media-app

Media Manifest File Statistics
-----------------------
Preposition Hit                                       :                0
Alien Hit                                             :                0
Cache Hit                                             :                0
Cache Miss                                            :                0
Partial Cache Hit                                     :                0
Cache Bypass                                          :                0

Media Fragment File Statistics
-----------------------
Preposition Hit                                       :                0
Alien Hit                                             :                0
Cache Hit                                             :                0
Cache Miss                                            :                0
Partial Cache Hit                                     :                0
Cache Bypass                                          :                0

Media Detail Statistics
----------------------
Active Assets                                         :                0
Active Manifest Files                                 :                0
Active Media Files                                    :                0
Request Sent To Default App                           :                0

Session Statistics
----------------------
Active Media sessions                                 :                0
Sessions Created                                      :                0
Sessions Created-Internal SessID                      :                0
Sessions Recreated With Received Cookie               :                0
Sessions Deleted-Inactive                             :                0
Sessions Deleted-Internal Error                       :                0
Sessions Deleted-Expired Request                      :                0
Sessions Deleted-Session ID Error                     :                0
Requests Rejected-Client IP Invalid                   :                0
```

```
Requests Rejected-SessID Collision                    :                 0
Requests Rejected-Failed to Track                     :                 0
Inline Key Requests                                   :                 0
Start Notifications sent                              :                 0
Start Notification send failed                        :                 0
Stop Notifications sent                               :                 0
Stop Notification send failed                         :                 0
Notification message send aborted due to DNS failure  :                 0
ServiceEngine#
```

The following example shows how to display the detailed statistics for the Zeri-Media-App:

```
ServiceEngine# show statistics web-engine abr zeri-media-app detail

Media Detail Statistics
-----------------------
Active DataSource              :                        0
Request Sent To Default App    :                        0
ServiceEngine#
```

The following example shows how to display the summary for the Smooth-Media-App:

```
ServiceEngine# show statistics web-engine abr smoothhd-media-app summary

Media Summary Statistics
------------------------
Preposition Hit                :                        0
External Hit                   :                        0
Cache Hit                      :                        0
Cache Miss                     :                        0
ServiceEngine#
```

Related Commands

Command	Description
show web-engine	Displays the Web Engine information.
web-engine (EXEC)	Configures the Web Engine module.
web-engine (global configuration)	Configures the Web Engine caching parameters.

show tacacs

To display Terminal Access Controller Access Control System Plus (TACACS+) authentication protocol configuration information, use the **show tacacs** command in EXEC configuration mode.

show tacacs

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **show tacacs** command displays the TACACS+ configuration for the Service Engine.

Table 2-65 describes the fields shown in the **show tacacs** display.

Table 2-65 show tacacs Field Descriptions

Field	Description
Login Authentication for Console/Telnet Session	Status of whether TACACS+ server is enabled for login authentication.
Configuration Authentication for Console/Telnet Session	Status of whether TACACS+ server is enabled for authorization or configuration authentication.
Authentication scheme fail-over reason	Status of whether Service Engines fails over to the secondary method of administrative login authentication whenever the primary administrative login authentication method is used.
TACACS+ Configuration	TACACS+ server parameters.
TACACS+ Authentication	Status of whether TACACS+ authentication is enabled on the Service Engine.
Key	Secret key that the Service Engine 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).
Timeout	Number of seconds that the Service Engine waits for a response from the specified TACACS+ Authentication Server before declaring a timeout.
Retransmit	Number of times that the Service Engine is to retransmit its connection to the TACACS+ server if the TACACS+ timeout interval is exceeded.
Password type	Mechanism for password authentication. By default, the Password Authentication Protocol (PAP) is the mechanism for password authentication.

Table 2-65 show tacacs Field Descriptions (continued)

Field	Description
Server	Hostname or IP address of the TACACS+ server.
Status	Status of whether server is the primary or secondary host.

Related Commands

Command	Description
clear tacacs	Clears the TACACS+ settings.
show statistics tacacs	Displays the SE TACACS+ authentication and authorization statistics.
tacacs	Configures TACACS+ server parameters.

show tech-support

To view information necessary for the Cisco Technical Assistance Center (TAC) to assist you, use the **show tech-support** command in EXEC configuration mode.

show tech-support [**list-files** *directory_name* [**recursive**] | **page** | **service** {**authentication** | **cms** | **kernel** | **web-engine**] | **authentication**}]

Syntax Description

list-files	(Optional) Displays the list of files under a directory.
directory_name	Directory name (use absolute path, such as /local1/logs).
recursive	Specifies to include files in recursive sub-directories.
page	(Optional) Specifies the pages through the output.
service	(Optional) Displays technical support information specific to a service.
authentication	Displays technical support information related to HTTP authentication.
cms	Displays technical support information related to CMS.
kernel	Displays technical support information related to the kernel.
web-engine	Displays technical support information related to the Web Engine.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use this command to view system information necessary for TAC to assist you with your SE. We recommend that you log the output to a disk file. Use the streaming option to view information specific to the streaming feature.

You can access the following general information when you enter the **show tech-support** command:

- Version and hardware (**show version**)
- Running configuration (**show running-config**)
- Processes (**show processes**)
- Process memory (**show processes memory**)
- System memory
- File system information
- Interface information
- Media file system statistics
- Application and kernel core dump information
- Netstat

Examples

The following example shows the types of information available about the CDS software. Because the **show tech-support** command output is comprehensive and can be extensive, only excerpts are shown in the following example:

```
ServiceEngine# show tech-support

CPU Usage:
   cpu: 0.39% User,  0.42% System,  0.33% User(nice),  98.86% Idle
  cpu0: 0.39% User,  0.42% System,  0.33% User(nice),  98.86% Idle
------------------------------------------------------------------------
 PID  STATE PRI User T  SYS T        COMMAND
----- ----- --- ------ ------ --------------------
    1     S   0   4386   1706 (init)
    2     S   0      0      0 (keventd)
    3     S  19      0      0 (ksoftirqd_CPU0)
    4     S   0      0      0 (kswapd)
    5     S   0      0      0 (bdflush)
    6     S   0      0      0 (kupdated)
    7     S   0      0      0 (scsi_eh_0)
   45     S   0   4733   4114 (nodemgr)
   46     S   0      0      0 (syslogd)
   47     R   0     83     65 (dataserver)
  920     S   0      0      0 (login)
 1207     S   0      0      0 (parser_server)
 1208     S   0      0      0 (eval_timer_mana)
 1211     S   0     46      1 (parser_server)
 1443     S   0      0      0 (overload)
 1444     S   0      0      0 (standby)
 1445     S   0     13     29 (cache)
 1446     S   0      0      0 (proxy_poll)
 1447     S   0      0      0 (snmpced)
 1448     S   0      0      0 (http_authmod)
 1458     S   0      0      0 (http_authmod)
 1465     S   0      0      0 (http_authmod)
 1466     S   0      0      0 (http_authmod)
 1467     S   0      0      0 (http_authmod)
 1537     S   0      0      0 (cache)
 1538     S   0      0      0 (unified_log)
 1540     S   0      0      1 (webserver)
 1541     S   0      2      2 (mcm)
 1542     S   0      0      0 (cache)
 1543     S   0      0      0 (cache)
 1550     S   0      0      0 (cache)
 1551     S   0      0      0 (cache)
 1556     S   0      0      0 (cache)
 1567     S   0      0      0 (mcm)
 1568     S   0      0      0 (mcm)
 1629     S   0  18982   4140 (crond)
 1936     S   0   1669    611 (bootnet)
 1937     S  10      0      0 (tracknet)
 1938     S  10  33545   5556 (checkup)
 1983     S   0      0      0 (srcpd)
 2023     S   0      1      0 (admin-shell)
 2024     S   0      0      0 (parser_server)
 2150     S   0      0      0 (rsvpd)
 2152     S   0      0      0 (rtspd)
 2153     S   0   1635   1067 (httpsd)
 2164     S   0      0      0 (librarian)
 2167     S   0   1667   2105 (libaux)
 2170     S   0      0      0 (mapper)
 2178     S   0     32     37 (cache)
 2179     S   0      0      0 (router)
 2180     S   0      0      0 (fill)
```

```
 2183    S   0      0      0 (remotereq)
 2185    S -20      0      0 (videosvr)
 2188    S   0      9      4 (contentsvr)
 2189    S   0      0      0 (routeraux)
 2190    S   0      0      1 (dfcontrolsvr)
 2226    S   0      0      0 (smbd)
 2228    S   0      0      0 (nmbd)
 2973    Z   0      0      0 (cache)
 8446    S   0      0      0 (httpsd)
 8447    S   0      0      0 (gcache)
18173    S   0      0      0 (in.telnetd)
18174    S   0      0      0 (login)
18175    S   0      2      2 (admin-shell)
18176    S   0      0      0 (parser_server)
19426    S   0      0      0 (httpsd)
19427    S   0      0      0 (httpsd)
19456    Z   0      0      0 (cache)
19503    Z   0     30      3 (crond)
19515    S   0      0      0 (more)
19516    S   0      6     18 (exec_show_tech-)
19553    R   0      0      0 (exec_show_proce)

------------------ process memory --------------------

     Total       Used       Free     Shared    Buffers     Cached
1050943488  564785152  486158336          0    5222400  475176960



   PID State    TTY  %MEM    VM Size RSS (pages) Name
------ ----- ------ ----- ---------- ----------- ----
     1     S      0  0.0    1146880         119 (init)
     2     S      0  0.0          0           0 (keventd)
     3     S      0  0.0          0           0 (ksoftirqd_CPU0)
     4     S      0  0.0          0           0 (kswapd)
     5     S      0  0.0          0           0 (bdflush)
     6     S      0  0.0          0           0 (kupdated)
     7     S      0  0.0          0           0 (scsi_eh_0)
    45     S      0  0.0    1208320         143 (nodemgr)
    46     S      0  0.0    1630208         194 (syslogd)
    47     R      0  0.0    1974272         238 (dataserver)
   920     S   1088  0.0    1728512         236 (login)
  1207     S      0  0.3    4980736         847 (parser_server)
  1208     S      0  0.0    1933312         151 (eval_timer_mana)
  1211     S      0  0.3    4980736         847 (parser_server)
  1443     S      0  0.0    1548288         154 (overload)
  1444     S      0  0.0    1724416         161 (standby)
  1445     S      0  5.9   65646592       15266 (cache)
  1446     S      0  0.0    1957888         173 (proxy_poll)
  1447     S      0  0.1    2097152         290 (snmpced)
  1448     S      0  0.0    1757184         205 (http_authmod)
  1458     S      0  0.0    1757184         205 (http_authmod)
  1465     S      0  0.0    1757184         205 (http_authmod)
  1466     S      0  0.0    1757184         205 (http_authmod)
  1467     S      0  0.0    1757184         205 (http_authmod)
  1537     S      0  5.9   65646592       15266 (cache)
  1538     S      0  0.0    1789952         169 (unified_log)
  1540     S      0  0.4   10817536        1164 (webserver)
  1541     S      0  0.0    2150400         251 (mcm)
  1542     S      0  5.9   65646592       15266 (cache)
  1543     S      0  5.9   65646592       15266 (cache)
  1550     S      0  5.9   65646592       15266 (cache)
  1551     S      0  5.9   65646592       15266 (cache)
```

```
  1556     S      0  5.9   65646592       15266 (cache)
  1567     S      0  0.0    2150400         251 (mcm)
  1568     S      0  0.0    2150400         251 (mcm)
  1629     S      0  0.0    1187840         137 (crond)
  1936     S      0  0.6    7532544        1605 (bootnet)
  2189     S      0  0.3    6103040         953 (routeraux)
  2190     S      0  0.4   10272768        1075 (dfcontrolsvr)
  2226     S      0  0.1    3559424         504 (smbd)
  2228     S      0  0.0    2084864         247 (nmbd)
  2973     Z      0  0.0          0           0 (cache)
  8446     S      0  0.1    2506752         327 (httpsd)
  8447     S      0  0.0    1421312         116 (gcache)
 18173     S      0  0.0    1220608         132 (in.telnetd)
 18174     S  34816  0.0    1736704         238 (login)
 18175     S  34816  0.0    2162688         184 (admin-shell)
 18176     S      0  0.3    4980736         847 (parser_server)
 19426     S      0  0.1    2551808         350 (httpsd)
 19427     S      0  0.1    2576384         354 (httpsd)
 19456     Z      0  0.0          0           0 (cache)
 19503     Z      0  0.0          0           0 (crond)
 19515     S  34816  0.0    1163264         109 (more)
 19516     S  34816  0.0    1941504         168 (exec_show_tech-)
 19554     R  34816  0.1    2277376         266 (exec_show_proce)

------------------ system memory --------------------

Total physical memory    :    1026312 KB
Total free memory        :     474692 KB
Total memory shared      :          0 KB
Total buffer memory      :       5100 KB
Total cached memory      :     464040 KB

------------------ interfaces --------------------

Interface type: GigabitEthernet Slot: 0 Port: 0
Type:Ethernet
Ethernet address:00:05:32:02:DD:74
Internet address:172.16.5.234
Netmask:255.255.255.0
Maximum Transfer Unit Size:1500
Metric:1
Packets Received: 513241
Input Errors: 0
Input Packets Dropped: 0
Input Packets Overruns: 0
Input Packets Frames: 0
Packet Sent: 153970
Output Errors: 0
Output Packets Dropped: 0
Output Packets Overruns: 0
Output Packets Carrier: 0
Output Queue Length:100
Collisions: 0
Interrupts:9
MULTICASTMode:autoselect, 100baseTX
```

show telnet

To display the Telnet services configuration, use the **show telnet** command in EXEC configuration mode.

show telnet

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled.

Command Modes

EXEC configuration mode.

Examples

The following example shows how to display the Telnet service details:

```
ServiceEngine# show telnet
telnet service is enabled
```

Related Commands

Command	Description
exec-timeout	Configures the length of time that an inactive Telnet or SSH session remains open.
telnet enable	Enables the Telnet services.

show transaction-logging

To display the transaction log configuration settings and a list of archived transaction log files, use the **show transaction-logging** command in EXEC configuration mode.

show transaction-logging

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

To display information about the current configuration of transaction logging on an SE, use the **show transaction-logging** command. Transaction log file information is displayed for HTTP caching proxy transactions and Trivial File Transfer Protocol (TFTP) and Internet Content Adaptation Protocol (ICAP) transactions.

Examples

The following example shows how to display information about the current configuration of transaction logging on an SE:

```
ServiceEngine# show transaction-logging
Transaction log configuration:
---------------------------------------
Logging is enabled.
Archive interval: 1800 seconds
Maximum size of archive file: 2000000 KB
Maximum number of archive files: 50 files
Log File format is apache.
Windows domain is not logged with the authenticated username

Exporting files to ftp servers is enabled.
File compression is disabled.
Export interval: 30 minutes

server               type  username        directory
10.77.153.110        ftp   root            /var/ftp/test

A&D Transaction Log File Info
  Working Log file - size : 138
                     age: 483497
  Archive Log file - acqdist_3.1.18.8_20090522_074807   size: 138
ICAP Transaction Log File Info
  Working Log file - size : 61
                     age: 483496
  Archive Log file - icap_3.1.18.8_20090522_074807      size: 61

Web Engine Transaction Log File Info - Apache format
  Working Log file - size : 86
                     age: 483497
  Archive Log file - we_accesslog_apache_3.1.18.8_20090522_074807       size: 82
```

```
Web Engine Transaction Log File Info - CLF format
  Working Log file - size : 3
                     age: 483497
  Archive Log file - we_accesslog_clf_3.1.18.8_20090522_074807 size: 3

Web Engine Transaction Log File Info - Extended Squid format
  Working Log file - size : 102
                     age: 483497
  Archive Log file - we_accesslog_extsqu_3.1.18.8_20090522_074807       size: 10
2

Cached Content Log File Info
  Working Log file - size : 41
                     age: 483496
  Archive Log file - cache_content_3.1.18.8_20090522_074807     size: 41

Authserver Transaction Log File Info
  Working Log file - size : 108
                     age: 483496
  Archive Log file - authsvr_3.1.18.8_20090522_065857   size: 108
ServiceEngine#
```

The following example shows how to display information about the current configuration of transaction logging on an SR:

```
ServiceRouter# show transaction-logging
Transaction log configuration:
--------------------------------------
Logging is enabled.
Archive interval: 120 seconds
Maximum size of archive file: 2000000 KB
Maximum number of archive files: 50 files

Exporting files to ftp servers is enabled.
File compression is disabled.
Export interval: 1 minute

server               type   username        directory
10.74.115.12         sftp   xinwwang        /workspace/xinwwang/test
10.74.124.156        sftp   root            /root/test
10.74.124.157        sftp   root            /root/test
171.71.50.162        sftp   root            /test

Service Router Log File Info
  Working Log file - size : 96
                     age: 169813
  Archive Log file - service_router_3.1.14.70_20090421_222006   size: 256
  Archive Log file - service_router_3.1.14.70_20090422_020038   size: 223
  Archive Log file - service_router_3.1.14.70_20090422_210022   size: 351
  Archive Log file - service_router_3.1.14.70_20090423_020006   size: 1248
  Archive Log file - service_router_3.1.14.70_20090423_210021   size: 456
  Archive Log file - service_router_3.1.14.70_20090521_000218   size: 402
  Archive Log file - service_router_3.1.14.70_20090521_014815   size: 243
  Archive Log file - service_router_3.1.14.70_20090521_015020   size: 225
  Archive Log file - service_router_3.1.14.70_20090521_015227   size: 243
  Archive Log file - service_router_3.1.14.70_20090521_015417   size: 272
  Archive Log file - service_router_3.1.14.70_20090521_015601   size: 390
  Archive Log file - service_router_3.1.14.70_20090521_015816   size: 243
  Archive Log file - service_router_3.1.14.70_20090521_020033   size: 243
  Archive Log file - service_router_3.1.14.70_20090521_020249   size: 143
  Archive Log file - service_router_3.1.14.70_20090521_032633   size: 168
  Archive Log file - service_router_3.1.14.70_20090526_025027   size: 143
  Archive Log file - service_router_3.1.14.70_20090526_030002   size: 176
```

```
Archive Log file - service_router_3.1.14.70_20090526_030226   size: 250
Archive Log file - service_router_3.1.14.70_20090526_052206   size: 250
Archive Log file - service_router_3.1.14.70_20090526_052413   size: 143
Archive Log file - service_router_3.1.14.70_20090526_200213   size: 168
Archive Log file - service_router_3.1.14.70_20090526_200413   size: 481
Archive Log file - service_router_3.1.14.70_20090526_200645   size: 173
Archive Log file - service_router_3.1.14.70_20090526_201010   size: 250
```

Related Commands

Command	Description
clear transaction-log	Clears the working transaction log settings.
show statistics transaction-logs	Displays the SE transaction log export statistics.
transaction-log force	Forces the archive or export of the transaction log.

show url-signature

To display the URL signature information, use the **show url-signature** command in EXEC configuration mode.

show url-signature

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to display the URL signature information:

```
ServiceEngine# show url-signature
key-id-owner key-id-number key
------------------------------
```

show user

To display the user identification number and username information for a particular user, use the **show** command in EXEC configuration mode.

show user {**uid** *num* | **username** *name*}

Syntax Description

uid	Displays the user's identification number.
num	Identification number. The range is from 0 to 65535.
username	Displays the name of user.
name	Name of the user.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-66 describes the fields shown in the **show user** display.

Table 2-66 show user Field Descriptions

Field	Description
Uid	User ID number.
Username	Username.
Password	Login password. This field does not display the actual password.
Privilege	Privilege level of the user.
Configured in	Database in which the login authentication is configured.

Related Commands

Command	Description
clear user	Clears the user settings.
show users	Displays the specified users.
username	Establishes the username authentication.

show users

To display users, use the **show users** command in EXEC configuration mode.

show users administrative

Syntax Description

administrative	Lists users with administrative privileges.

Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to display the list of users with administrative privileges:

```
ServiceEngine# show users administrative
           UID USERNAME
           0 admin
```

Related Commands

Command	Description
clear user	Clears the user settings.
show user	Displays the user identification number and username information for a particular user.
username	Establishes the username authentication.

show version

To display version information about the software, use the **show version** command in EXEC configuration mode.

show version pending

Syntax Description

pending	Displays the version for pending upgraded image.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-67 describes the fields shown in the **show version** display.

Table 2-67 show version Field Descriptions

Field	Description
Version	VDS-OS software version.
Compiled hour:minute:second month day year by cnbuild	Compile information for the software build.
System was restarted on day of week month day hour:minute:second year	Date and time that the system was last restarted.
The system has been up for X hours, X minutes, X seconds	Length of time the system has been running since the last reboot.

Note If you update the VDS-OS software on an SE, the new version displays in the **show version pending** command output, but it says, "Pending version will take effect after reload." You must reboot the device for the software update to take affect.

Examples

The follow example shows how to display the software version:

```
ServiceEngine# show version
Videoscape Distribution Suite Origin Server Software
Copyright (c) 1999-2011 by Cisco Systems, Inc.
Content Delivery System Software Release 3.0.0 (build b460 Aug 28 2011)
Version: cde220-2g2-DEVELOPMENT[vcn-build1:/auto/vcn-u1/vosis_release_builds/vos
is_3.0.0-b460/spcdn]

Compiled 05:55:01 Aug 28 2011 by ipvbuild
Compile Time Options: KQ SS

System was restarted on Mon Aug 29 11:56:58 2011.
The system has been up for 1 day, 23 hours, 32 minutes, 15 seconds.
```

```
ServiceEngine#
```

The following example shows how to display the pending software version:

```
ServiceEngine# show version pending
Pending version is VDS-OS 3.0.0-b360, built on 05:17:52 Jun 19 2011 by ipvbuild
It will take effect after reload
ServiceEngine#
```

Related Commands

Command	Description
show flash	Displays the flash memory version and usage information.

show vos

To display Videoscape Distribution Suite Origin Server (VDS-OS) information about the software, use the **show vos** command in EXEC configuration mode.

show vos {**asset** *livePublishResrcName* | **capture-src-manager** {**channels** | **statistics**} | **channel** {**all** | *channelURI* [**config** [**outfile** *filename*]] | **schedule** [**all** [**outfile** *filename*] | [*publishResrcName*]] | **origin-service** [**all** | *srdn*]}}

Syntax Description

asset *livePublishResrcName*	Displays the asset information for the specified live publish resource. **Note** The **asset** keyword is not supported in VDS-OS 2.0.
capture-src-manager	Displays the CapturesourceManager information. **Note** The **capture-src-manager** keyword is not supported in VDS-OS 2.0.
channels	Displays all CapturesourceManager channels. **Note** The **channels** keyword is not supported in VDS-OS 2.0.
statistics	Displays all CapturesourceManager statistics. **Note** The **statistics** keyword is not supported in VDS-OS 2.0.
channel	Displays the channel information.ch
all	Displays the status of all channels.
channelURI	Displays information specific to channel URI.
config	Displays the channel configuration details.
outfile *filename*	Specifies redirect output to file *filename*.
schedule	Displays the status of the active live and capture events.
all	Displays the status of all active live and capture events.
publishResrcName	Publish resource URI.
origin-service	Displays Origin Services information.
all	Displays the list of Origin Services.
srdn	Displays the general settings of the origin-service identified by the Service Routing Domain Name (SRDN).

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **show vos asset** *livePublishResrcName* command displays the following information for the Live Publish Resource:

- Channel ID
- Publish URI
- Acquisition Node

- Asset Path
- For each bit rate:
  - How many segments are available on the disk
  - How many segments are available on the playlist Manifest file
  - Total Segment duration in the Manifest

The **show vos origin-service all** command displays the list of Origin Services. When this command is issue, the CLI sends HTTP request to the Capture Controller:

```
GET /vosapi/CaptureController/OriginService/
VOS-CMD-HDR: ShowVosOriginServiceAll
```

The **show vos origin-service** *srdn* command displays the general settings of the origin-service identified by the SRDN. When this command is issued, the CLI looks up the configuration from the Data Server.

The **show vos channel all** command displays the channel URI and status of all the channels on the box. When this command is issued, the CLI sends the following HTTP request to the Capture Controller:

```
GET /vosapi/CaptureController/ChannelMgr/List HTTP/1.0
User-Agent: Wget/1.12 (linux-gnu)
Accept: */*
Host: 127.0.0.1:8080
Connection: Keep-Alive
```

The **show vos channel** *channelURI* command displays the following information for the channel specified by channel URI:

- State of the Channel
- Capture Resource - URLs, State, CaptureStream (IDs and state)
- Live Publish Resource - URL, State
- Num. Active Capture Events

When this command is issued, the CLI sends the following HTTP request to the Capture Controller:

```
GET /vosapi/CaptureController/ChannelMgr/abchd_east/Details HTTP/1.0
User-Agent: Wget/1.12 (linux-gnu)
Accept: */*
Host: vos.sp.net
Connection: Keep-Alive
```

The **show vos channel** *channelURI* **config** command displays the Channel Config Extensible Markup Language (XML) in a user-friendly format. When this command is issued, the CLI displays the XML by looking up the file path from the Data Server.

The **show vos channel** *channelURI* **schedule** command displays all the publish URIs and the state of all the active publish and capture events for the channel specified by *channelURI*. When this command is issued, the CLI sends the following HTTP request to the Capture Controller:

```
GET /vosapi/CaptureController/ChannelMgr/abchd_east/ScheduleActive HTTP/1.0
User-Agent: Wget/1.12 (linux-gnu)
Accept: */*
Host: vos.sp.net
Connection: Keep-Alive
```

The **show vos channel** *channelURI* **schedule all** command displays the publish URI and the state of all the events for the channel specified by *channelURI*. When this command is issued, the CLI sends the following HTTP request to the Capture Controller:

```
GET /vosapi/CaptureController/ChannelMgr/abchd_east/ScheduleAll HTTP/1.0
User-Agent: Wget/1.12 (linux-gnu)
```

```
Accept: */*
Host: vos.sp.net
Connection: Keep-Alive
```

The **show vos channel** *channelURI* **schedule** *publishResrcName* command displays the following information for the Publish Resource or the Capture Event:

- Format - HLS/HSS
- State of the Publish Resource/Capture Event
- Publish URL, StartOverURL (if applicable)
- Schedule - Start Time & End Time
- Capture Resource & Capture Stream Information - URI, State
- Action on Completion (if applicable)
- TimeShiftBuffer (if applicable)

When this command is issued, the CLI sends the following HTTP request to the Capture Controller:

```
GET/vosapi/CaptureController/ChannelMgr/abchd_east/PublishResource/hd/all/live/hls/index.m
3u8/Details HTTP/1.0
User-Agent: Wget/1.12 (linux-gnu)
Accept: */*
Host: vos.sp.net
Connection: Keep-Alive
```

Examples

The follow example shows how to display the VDS-OS asset information for the Live Publish Resource:

```
ServiceEngine# show vos asset http://live.passthrough.com/live7/cap7/hls/index.m3u8

Channel ID      : http://live.passthrough.com/live7
Publish URI     : cap7/hls/index.m3u8

Acq. Node  : 37.0.116.199
Asset
Path :/state/export/NAS/live.passthrough.com/sharmi/mountpoint/0/o/live.passthrough.com/_S
ERVER_37.0.116.199/live7/cap7/hls
Profile       Duration       SegmentInManifest   SegmentOnStorage
=======       =========       =================   ================
strm4         27195                   4528            7617
strm3         27195                   4528            7078

strm2         27195                   4528            8858
strm1         27201                   4529            7600
```

The follow example shows how to display the VDS-OS capture-src-manager information:

```
ServiceEngine# show vos capture-src-manager channels

 ------------------------------------------------
   Number of Post Received           =  0
   Total DataBlock consumed          =  0
   Current DataBlock state           =  0
   Total DataBlockFactory Mem created=  0
```

The follow example shows how to display the VDS-OS capture-src-manager statistics:

```
ServiceEngine# show vos capture-src-manager statistics

 ----------------------Statistics----------------------------------------
   Average Time between Segment Arrival (usec)   =  0
```

```
   Maximum Time between Segment Arrival (usec)   =  0
   Minimum Time between Segment Arrival (usec)   =  0
```

The follow example shows how to display all VDS-OS channel information:

```
ServiceEngine# show vos channel all
Fetching...
Channel URI, Status:
--------------------
http://xxxx.test.com/Test-Live    Stopped
http://xxxx.test.com/Test-Live2    Stopped
http://xxxx.test.com/Test-live3    Stopped
http://vos.hls.com/bugverification    Stopped
```

The follow example shows how to display all VDS-OS information:

```
ServiceEngine# show vos origin-service all
Fetching...
Origin Services
---------------
vod.hss.com
vos.hls.com
vod.hds.com
sylvia.test.com
my.mickjagger.com

Total No. of Origin Services: 5
```

Related CommandsS

Command	Description
show statistics vos	Displays the VDS-OS statistics.

show web-engine

To display the Web Engine information, use the **show web-engine** command in EXEC configuration mode.

show web-engine {**all** | **admission-control** | **health** | **mediaapp**}

Syntax Description

all	Displays all Web Engine-related caching information.
admission-control	Displays the Web Engine admission control information.
health	Displays the Web Engine health information.
mediaapp	Displays the Web Engine media application information.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Because admission control CPU and RAM averages are weighted, their values might not be equivalent to values reported by other CLI.

Examples

The following example shows how to display the Web Engine information:

```
ServiceEngine# show web-engine all
HTTP heuristic age-multipliers: 30%

HTTP Body Read Buffer Size: 32 (KB)

Maximum time to live in days: 61

Minimum time to live in minutes: 60

Web Engine Maximum Concurrent Sessions: 20000

Web Engine OS certificate validation Enabled.
```

The following example shows how to display the Web Engine health information:

```
ServiceEngine# show web-engine health

WebEngine - Virtual memory Usage
---------------------------------
Total memory usage                    :          4603785216 bytes [UnderLimit]
Platform Virtual memory ThresHold     :          67473127424 bytes
Glibc Caching Turn-Off Threshold      :          40483876454 bytes
Glibc memory Caching                  :                   ON

Web Engine - Alarm Status
-------------------------
memory_exceeded                       :                  OFF
max_session_exceeded                  :                  OFF
WebCalLookupThreshold                 :                  OFF
```

```
WebCalDiskWriteThreshold                :                  OFF
aug_memory_exceeded                     :                  OFF
aug_session_exceeded                    :                  OFF
WebCalLookupAugThreshold                :                  OFF
WebCalDiskWriteAugThreshold             :                  OFF
UNKNOWN                                 :                  OFF
CMESyncFailed                           :                  OFF
CMEIndexDegraded                        :                  OFF
Overloaded                              :                  OFF
```

The following example shows how to display the Web Engine admission control information:

```
ServiceEngine# show web-engine admission-control

Assets Active                           :                    8
Assets Active Average                   :               19.515
Assets Blocked                          :                    0
Assets Blocked / Second Average         :                0.000
Estimated Max Active Assets             :               3704.5

Sessions Active                         :                    0
Sessions Active Average                 :                0.503
Sessions Blocked                        :                    0
Sessions Blocked / Second Average       :                0.000
Estimated Max Active Sessions           :               3704.5

CPU Utilization                         :                2.429 %
CPU Utilization Threshold               :               90.000 %
CPU Asset Weight                        :                0.024
CPU Session Weight                      :                0.024

RAM Utilization                         :                1.756 %
RAM Utilization Threshold               :               90.000 %
RAM Asset Weight                        :                0.018
RAM Session Weight                      :                0.018

CPU Averaging Weights                   :          0.750,0.250
RAM Averaging Weights                   :          0.750,0.250
Asset Weighting Threshold               :                  100
Session Weighting Threshold             :                  100

Overloaded                              :                   No
```

The following example shows how to display the Web Engine media application information:

```
ServiceEngine# show web-engine mediaapp

HLSMediaApp Stats: (0x7fde78274e00)
  MediaAssetHandler (0x7fde7826da80): No of Assets: 1
    MediaAsset (0x7fdde8041fc0): Asset URL
     (http://vos.ipndvr.com/58.0.118.109/ndvr/ip/824/hls) No of Media Profiles: 2
    MediaProfile (0x7fdde810f440): Profile URL
     (http://vos.ipndvr.com/58.0.118.109/ndvr/ip/824/hls/1614740) No of Media Files: 2
      MediaFile (0x7fdde800b500), MediaFileURL
       (http://vos.ipndvr.com/58.0.118.109/ndvr/ip/824/hls/1614740) MediaIndexTableUsed: 1
      HLSMediaManifest (0x7fdde810c5b0), ManifestFileURL
       (http://vos.ipndvr.com/58.0.118.109/ndvr/ip/824/hls/1614740.m3u8)
    MediaProfile (0x7fdde8043190): Profile URL
     (http://vos.ipndvr.com/58.0.118.109/ndvr/ip/824/hls/index) No of Media Files: 1
      HLSMediaManifest (0x7fdde8043410), ManifestFileURL
       (http://vos.ipndvr.com/58.0.118.109/ndvr/ip/824/hls/index.m3u8)
```

Related Commands

Command	Description
web-engine (EXEC)	Configures the Web Engine module.
web-engine (global configuration)	Configures the Web Engine caching parameters.
show statistics web-engine	Displays the Web Engine statistics.

shutdown (interface configuration)

To shut down a specific hardware interface, use the **shutdown** command in interface configuration mode. To restore an interface to operation, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Interface configuration (config-if) mode.

Usage Guidelines

See the "interface" section on page 2-112 for alternative mechanism.

Examples

The following example shows how to shut down an interface configured on an SE:

```
ServiceEngine(config-if)# shutdown
```

Related Commands

Command	Description
interface	Configures a Gigabit Ethernet or port channel interface.
show interface	Displays the hardware interface information.
show running-config	Displays the current operating configuration.
show startup-config	Displays the startup configuration.

shutdown (EXEC configuration)

To shut down the SE, SR or VOSM, use the **shutdown** command in EXEC configuration mode.

shutdown [**poweroff**]

Syntax Description

poweroff	(Optional) Turns off the power after closing all applications and the operating system.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

A controlled shutdown refers to the process of properly shutting down an SE without turning off the power on the device. With a controlled shutdown, all the application activities and the operating system are properly stopped on an SE but the power is still on. Controlled shutdowns of an SE can help you minimize the downtime when the SE is being serviced.

The **shutdown** command enables you to shut down and optionally power off an SE:

- *Shutdown* means that all application activities (applications and operating system) are stopped, but the power is still on. This shutdown is similar to the Linux **halt** command.
- *Shutdown poweroff* means that the SE is powered down by the VDS-OS software after being shut down. This operation is also referred to as a software poweroff. The implementation of the shutdown poweroff feature uses the Advanced Configuration and Power Interface (ACPI) power management interface.

Caution If you do not perform a controlled shutdown, the SE file system can be corrupted. It also takes longer to reboot the SE if the SE is not properly shut down.

Note You cannot power on SEs again through software after a software poweroff operation. You must press the power button once on these SEs to bring these SEs back online.

The **shutdown** command facilitates a proper shutdown for SEs, SRs, or VOSMs. Where the **shutdown** command is supported on all content networking hardware models, the **shutdown poweroff** command is supported only on those models that support ACPI.

The **shutdown** command closes all applications and stops all system activities but keeps the power on. The fans continue to run and the power LED is on, indicating that the device is still powered on. When you enter the **shutdown** command, you are prompted to save your configuration changes, if any. The device console displays a menu after the shutdown process is completed. You need to log in to the SE using a console to display the following menu:

```
ServiceEngine# shutdown
System configuration has been modified. Save? [ yes ] :yes
Device can not be powered on again through software after shutdown.
Proceed with shutdown? [ confirm ] yes
Shutting down all services, will timeout in 15 minutes.
shutdown in progress...Halt requested by CLI@ttyS0.
..........
Shutdown success

Cisco Service Engine Console

Username: admin
Password:

================= SHUTDOWN SHELL =================
   System has been shut down.

   You can either
      Power down system by pressing and holding power button
   or
   1. Reload system through software
   2. Power down system through software
   Please select [ 1-2 ] :
```

The **shutdown poweroff** command closes all applications and the operating system, stops all system activities, and turns off the power. The fans stop running and the power LED starts flashing, indicating that the device has been powered off.

Note If you use the **shutdown** or **shutdown poweroff** commands, the device does not perform a file system check when you power on and boot the device the next time.

Table 2-68 describes the shutdown and shutdown power-off operations for SEs.

Table 2-68 Shutting Down Content Engines Through CLI Commands

Activity	All Content Engine Models	Content Engines with Power Management Capability
User performs a shutdown operation on the SE	`ServiceEngine# shutdown`	`ServiceEngine# shutdown poweroff`
User intervention to bring SE back online	To bring an SE that has an on/off switch on the back online after a shutdown operation, flip the on/off switch twice. To bring an SE that has a power button (instead of an on/off switch on the back) back online after a shutdown operation, first press and hold the power button for several seconds to power off these models, and then press the power button once again.	After a shutdown poweroff, press the power button once to bring the SE back online.
File system check	Is not performed after you turn the power on again and reboot the SE.	Is not performed after you turn the power on again and reboot the SE.

You can enter the **shutdown** command from a console session or from a remote session (Telnet or SSH Version 1 or SSH Version 2) to perform a shutdown on an SE.

To perform a shutdown on an SE, enter the **shutdown** command as follows:

```
ServiceEngine# shutdown
```

When you are asked if you want to save the system configuration, enter **yes** as follows:

```
System configuration has been modified. Save? [ yes ] :yes
```

When you are asked if you want to proceed with the shutdown, press **Enter** to proceed with the shutdown operation as follows:

```
Device can not be powered on again through software after shutdown.
Proceed with shutdown? [ confirm ]
```

The following message appears, reporting that all services are being shut down on this SE:

```
Shutting down all services, will timeout in 15 minutes.
shutdown in progress...System halted.
```

After the system is shut down (the system has halted), a VDS-OS software shutdown shell displays the current state of the system (for example, `System has been shut down`) on the console. You are asked whether you want to perform a software power off (the Power down system by software option), or if you want to reload the system through the software.

```
================= SHUTDOWN SHELL =================
System has been shut down.

You can either
   Power down system by pressing and holding power button
or
1. Reload system through software
2. Power down system through software
```

To power down the SE, press and hold the power button on the SE, or use one of the following methods to perform a shutdown poweroff:

- From the console command line, enter **2** when prompted as follows:

  ```
  ================= SHUTDOWN SHELL =================
  System has been shut down.
  You can either
     Power down system by pressing and holding power button
  or
  1. Reload system through software
  2. Power down system through software
  ```

- From the SE CLI, enter the **shutdown poweroff** command as follows:

  ```
  ServiceEngine#  shutdown poweroff
  ```

  When you are asked if you want to save the system configuration, enter **yes** as follows:

  ```
  System configuration has been modified. Save? [ yes ] :yes
  ```

  When you are asked to confirm your decision, press **Enter**.

  ```
  Device can not be powered on again through software after poweroff.
  Proceed with poweroff? [ confirm ]
  Shutting down all services, will timeout in 15 minutes.
  poweroff in progress...Power down.
  ```

Examples

The following example shows that the **shutdown** command is used to close all applications and stop all system activities:

```
ServiceEngine1# shutdown
System configuration has been modified. Save? [ yes ] :yes
Device can not be powered on again through software after shutdown.
Proceed with shutdown? [ confirm ]
Shutting down all services, will timeout in 15 minutes.
shutdown in progress...System halted.
```

The following example shows that the **shutdown poweroff** command is used to close all applications, stop all system activities, and then turn off power to the SE:

```
ServiceEngine2# shutdown poweroff
System configuration has been modified. Save? [ yes ] :yes
Device can not be powered on again through software after poweroff.
Proceed with poweroff? [ confirm ]
Shutting down all services, will timeout in 15 minutes.
poweroff in progress...Power down.
```

snmp-server community

To configure the community access string to permit access to the Simple Network Management Protocol (SNMP), use the **snmp-server community** command in global configuration mode. To remove the specified community string, use the **no** form of this command.

snmp-server community *community_string* [**group** *group_name* | **rw**]

no snmp-server community *community_string* [**group** *group_name* | **rw**]

Syntax Description

community_string	Community string that acts like a password and permits access to SNMP.
group	(Optional) Specifies the group to which this community name belongs.
group_name	(Optional) Name of the group.
rw	(Optional) Specifies read-write access with this community string.

Defaults

An SNMP community string permits read-only access to all Management Information Base (MIB) objects.

A community string is assigned to the Secure Domain Router (SDR) owner.

Command Modes

Global configuration (config) mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. Use the **snmp-server community** command to configure the community access string to permit access to SNMP. To remove the specified community string, use the **no** form of this command.

Note In a non-owner SDR, a community name provides access only to the object instances that belong to that SDR, regardless of the access privilege assigned to the community name. Access to the owner SDR and system-wide access privileges are available only from the owner SDR.

Examples

The following example shows how to add the community comaccess:

```
ServiceEngine(config)# snmp-server community comaccess rw
```

The following example shows how to remove the community comaccess:

```
ServiceEngine(config)# no snmp-server community comaccess
```

Related Commands

Command	Description
snmp-server view	Defines a Version 2 SNMP (SNMPv2) MIB view.

snmp-server contact

To set the system server contact (sysContact) string, use the **snmp-server contact** command in global configuration mode. To remove the system contact information, use the **no** form of this command.

snmp-server contact *line*

no snmp-server contact

Syntax Description

line	Identification of the contact person for this managed node.

Defaults

No system contact string is set.

Command Modes

Global configuration (config) mode.

Usage Guidelines

The system contact string is the value stored in the MIB-II system group sysContact object.

Examples

The following example shows how to configure a system contact string:

```
ServiceEngine(config)# snmp-server contact Dial System Operator at beeper # 27345
```

The following example shows how to reset the system contact string:

```
ServiceEngine(config)# no snmp-server contact
```

Related Commands

Command	Description
show snmp	Displays the SNMP parameters.
snmp-server community	Configures the community access string to permit access to the SNMP.
snmp-server enable traps	Enables the Service Engine (SE) to send SNMP traps.
snmp-server group	Defines a user security model group.
snmp-server host	Specifies the hosts to receive SNMP traps.
snmp-server location	Sets the SNMP system location string.
snmp-server notify inform	Configures the SNMP notify inform request.
snmp-server user	Defines a user who can access the SNMP engine.
snmp-server view	Defines a SNMPv2 MIB view.

snmp-server enable traps

To enable the Service Engine (SE) to send Simple Network Management Protocol (SNMP) traps, use the **snmp-server enable traps** command in global configuration mode. To disable all SNMP traps or only SNMP authentication traps, use the **no** form of this command.

snmp-server enable traps [**alarm** [**clear-critical** | **clear-major** | **clear-minor** | **raise-critical** | **raise-major** | **raise-minor**] | **config** | **entity** | **event** | **service-engine** [**disk-fail** | **disk-read** | **disk-write** | **transaction-log**] | **snmp** [**authentication** | **cold-start**]]

no snmp-server enable traps [**alarm** [**clear-critical** | **clear-major** | **clear-minor** | **raise-critical** | **raise-major** | **raise-minor**] | **config** | **entity** | **event** | **service-engine** [**disk-fail** | **disk-read** | **disk-write** | **transaction-log**] | **snmp** [**authentication** | **cold-start**]]

Syntax Description

alarm	(Optional) Enables SE alarm traps.
clear-critical	(Optional) Enables the clear-critical alarm trap.
clear-major	(Optional) Enables the clear-major alarm trap.
clear-minor	(Optional) Enables the clear-minor alarm trap.
raise-critical	(Optional) Enables the raise-critical alarm trap.
raise-major	(Optional) Enables the raise-major alarm trap.
raise-minor	(Optional) Enables the raise-minor alarm trap.
config	(Optional) Enables CiscoConfigManEvent traps.
entity	(Optional) Enables SNMP entity traps.
event	(Optional) Enables Event Management Information Base (MIB) traps.
service-engine	(Optional) Enables SNMP SE traps.
disk-fail	(Optional) Enables the disk failure error trap.
disk-read	(Optional) Enables the disk read error trap.
disk-write	(Optional) Enables the disk write error trap.
transaction-log	(Optional) Enables the transaction log write error trap.
snmp	(Optional) Enables SNMP-specific traps.
authentication	(Optional) Enables the authentication trap.
cold-start	(Optional) Enables the cold-start trap.

Defaults

This command is disabled by default. No traps are enabled.

Command Modes

Global configuration (config) mode.

Usage Guidelines

You can configure an SE to generate an SNMP trap for a specific alarm condition. You can configure the generation of SNMP alarm traps on SEs based on the following:

- Severity of the alarm (critical, major, or minor)
- Action (the alarm is raised or cleared)

VDS-OS software supports six generic alarm traps. These six generic alarm traps provide SNMP and Node Health Manager integration. Each trap can be enabled or disabled through the SE CLI.

Note Some SNMP traps are different between v1 and v2 and v3 when configure the trap.

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps** command enables both traps and inform requests for the specified notification types.

To configure traps, enter the **snmp-server enable traps** command. If you do not enter the **snmp-server enable traps** command, no traps are sent.

If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. To configure the SE to send these SNMP notifications, enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled. To enable multiple types of notifications, enter a separate **snmp-server enable traps** command for each notification type and notification option.

The **snmp-server enable traps** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP traps. To send traps, configure at least one host using the **snmp-server host** command.

For a host to receive a trap, enable both the **snmp-server enable traps** command and the **snmp-server host** command for that host.

In addition, enable SNMP with the **snmp-server community** command.

To disable the sending of the MIB-II SNMP authentication trap, enter the **no snmp-server enable traps snmp authentication** command.

Examples

The following example shows how to enable the Service Engine (SE) to send all traps to the host 172.31.2.160 using the community string public:

```
ServiceEngine(config)# snmp-server enable traps
ServiceEngine(config)# snmp-server host 172.31.2.160 public
```

The following example disables all traps:

```
ServiceEngine(config)# no snmp-server enable traps
```

Related Commands

Command	Description
show snmp	Displays the SNMP parameters.
snmp-server community	Configures the community access string to permit access to the SNMP.
snmp-server contact	Sets the system server contact string.
snmp-server group	Defines a user security model group.
snmp-server host	Specifies the hosts to receive SNMP traps.
snmp-server location	Sets the SNMP system location string.
snmp-server notify inform	Configures the SNMP notify inform request.
snmp-server user	Defines a user who can access the SNMP engine.
snmp-server view	Defines a SNMPv2 MIB view.

snmp-server group

To define a user security model group, use the **snmp-server group** command in global configuration mode. To remove the specified group, use the **no** form of this command.

snmp-server group *name* {**v1** [**notify** *name*] [**read** *name*] [**write** *name*] | **v2c** [**notify** *name*] [**read** *name*] [**write** *name*] | **v3** {**auth** [**notify** *name*] [**read** *name*] [**write** *name*] | **noauth** [**notify** *name*] [**read** *name*] [**write** *name*] | **priv** [**notify** *name*] [**read** *name*] [**write** *name*]}}

no snmp-server group *name* {**v1** [**notify** *name*] [**read** *name*] [**write** *name*] | **v2c** [**notify** *name*] [**read** *name*] [**write** *name*] | **v3** {**auth** [**notify** *name*] [**read** *name*] [**write** *name*] | **noauth** [**notify** *name*] [**read** *name*] [**write** *name*] | **priv** [**notify** *name*] [**read** *name*] [**write** *name*]}}

Syntax Description

name	Name of the Simple Network Management Protocol (SNMP) group. Supports up to a maximum of 64 characters.
v1	Specifies the group using the Version 1 Security Model.
notify	(Optional) Specifies a notify view for the group that enables you to specify a notify, inform, or trap.
name	Notify view name. Supports up to a maximum of 64 characters.
read	(Optional) Specifies a read view for the group that enables you only to view the contents of the agent.
name	Read view name. Supports up to a maximum of 64 characters.
write	(Optional) Specifies a write view for the group that enables you to enter data and configure the contents of the agent.
name	Write view name. Supports up to a maximum of 64 characters.
v2c	Specifies the group using the Version 2c Security Model.
v3	Specifies the group using the User Security Model (SNMPv3).
auth	Specifies the group using the AuthNoPriv Security Level.
noauth	Specifies the group using the noAuthNoPriv Security Level.
priv	Specifies the group using the AuthPriv Security Level.

Defaults

The default is that no user security model group is defined.

Command Modes

Global configuration (config) mode.

Usage Guidelines

The maximum number of SNMP groups that can be created is 10.

Select one of three SNMP security model groups: Version 1 (**v1**) Security Model, Version 2c (**v2c**) Security Model, or the User Security Model (**v3** or SNMPv3). Optionally, you then specify a notify, read, or write view for the group for the particular security model chosen. The **v3** option allows you to specify the group using one of three security levels: **auth** (AuthNoPriv Security Level), **noauth** (noAuthNoPriv Security Level), or **priv** (AuthPriv Security Level).

Note Each community is associated with a group. Each group has a view and users are assigned to a group. If the group does not have a view associated with it, then users associated that group cannot access any MIB entry.

The VDS-OS software supports the following versions of SNMP:

- Version 1 (SNMPv1)—This version is the initial implementation of SNMP. See RFC 1157 for a full description of its functionality.
- Version 2 (SNMPv2c)—This version is the second release of SNMP, described in RFC 1902. It provides additions to data types, counter size, and protocol operations.
- Version 3 (SNMPv3)—This version is the most recent SNMP version, defined in RFC 2271 through RFC 2275.

SNMP Security Models and Security Levels

SNMPv1 and SNMPv2c do not have any security (authentication or privacy) mechanisms to keep SNMP packet traffic on the wire confidential. As a result, packets on the wire can be detected and SNMP community strings can be compromised.

To solve the security shortcomings of SNMPv1 and SNMPv2c, SNMPv3 provides secure access to SEs by authenticating and encrypting packets over the network. The SNMP agent supports SNMPv3, SNMPv1, and SNMPv2c.

Using SNMPv3, users can securely collect management information from their SNMP agents. Also, confidential information, such as SNMP set packets that change an SE's configuration, can be encrypted to prevent their contents from being exposed on the wire. Also, the group-based administrative model allows different users to access the same SNMP agent with varying access privileges.

Examples

The following example shows how to configure the SNMP group name, security model, and notify view on the SE:

```
ServiceEngine(config)# snmp-server group acme v1 notify mymib
```

Related Commands

Command	Description
show snmp	Displays the SNMP parameters.
snmp-server community	Configures the community access string to permit access to the SNMP.
snmp-server contact	Sets the system server contact string.
snmp-server enable traps	Enables the Service Engine (SE) to send SNMP traps.
snmp-server host	Specifies the hosts to receive SNMP traps.
snmp-server location	Sets the SNMP system location string.
snmp-server notify inform	Configures the SNMP notify inform request.
snmp-server user	Defines a user who can access the SNMP engine.
snmp-server view	Defines a SNMPv2 MIB view.

snmp-server host

To specify the recipient of a host Simple Network Management Protocol (SNMP) trap operation, use the **snmp-server host** command in global configuration mode. To remove the specified host, use the **no** form of this command.

snmp-server host {*hostname* | *ip_address*} *communitystring* [**v2c** [**retry** *number*] [**timeout** *seconds*] | [**v3** {**auth** [**retry** *number*] [**timeout** *seconds*] | **noauth** [**retry** *number*] [**timeout** *seconds*] | **priv** [**retry** *number*] [**timeout** *seconds*]}]

no snmp-server host {*hostname* | *ip_address*} [**v2c** [**retry** *number*] [**timeout** *seconds*] | [**v3** {**auth** [**retry** *number*] [**timeout** *seconds*] | **noauth** [**retry** *number*] [**timeout** *seconds*] | **priv** [**retry** *number*] [**timeout** *seconds*]} | *communitystring*]

Syntax Description

hostname	Hostname of the SNMP trap host that is sent in the SNMP trap messages from the SE.
ip_address	IP address of the SNMP trap host that is sent in the SNMP trap messages from the SE.
communitystring	Password-like community string sent in the SNMP trap messages from the SE. You can enter a maximum of 64 characters.
v2c	(Optional) Specifies the Version 2c Security Model.
retry	(Optional) Sets the count for the number of retries for the inform request. (The default is 2 tries.)
number	Number of retries for the inform request. The range is from 1 to 10.
timeout	(Optional) Sets the timeout for the inform request The default is 15 seconds.
seconds	Timeout value, in seconds. The range is from 1 to 1000.
v3	(Optional) Specifies the User Security Model (SNMPv3).
auth	Sends notification using the AuthNoPriv Security Level.
noauth	Sends notification using the noAuthNoPriv Security Level.
priv	Sends notification using the AuthPriv Security Level.

Defaults

This command is disabled by default. No traps are sent. The version of the SNMP protocol used to send the traps is SNMP Version 1.

retry *number*: 2

timeout *seconds*: 15

Command Modes

Global configuration (config) mode.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Informs are more likely to reach their intended destination.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in the memory until a response is received or the request times out. Also, traps are sent only once, while an inform may be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the SE to send SNMP notifications, enter at least one **snmp-server host** command. To enable multiple hosts, enter a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of security model, each succeeding command overwrites the previous command. Only the last **snmp-server host** command is in effect. For example, if you enter an **snmp-server host v2c** command for a host and then enter another **snmp-server host v3** command for the same host, the second command replaces the first.

The maximum number of SNMP hosts that can be created by entering the **snmp-server host** commands is eight.

When multiple **snmp-server host** commands are given for the same host, the community string in the last command is used.

The **snmp-server host** command is used with the **snmp-server enable traps** command. Use the **snmp-server enable traps** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled.

Note You must enable SNMP with the **snmp-server community** command.

Examples

The following example sends the SNMP traps defined in RFC 1157 to the host specified by the IP address 172.16.2.160. The community string is comaccess:

```
ServiceEngine(config)# snmp-server enable traps
ServiceEngine(config)# snmp-server host 172.16.2.160 comaccess
```

The following example shows how to remove the host 172.16.2.160 from the SNMP trap recipient list:

```
ServiceEngine(config)# no snmp-server host 172.16.2.160
```

Related Commands

Command	Description
show snmp	Displays the SNMP parameters.
snmp-server community	Configures the community access string to permit access to the SNMP.
snmp-server contact	Sets the system server contact string.
snmp-server enable traps	Enables the Service Engine (SE) to send SNMP traps.
snmp-server group	Defines a user security model group.
snmp-server location	Sets the SNMP system location string
snmp-server notify inform	Configures the SNMP notify inform request.
snmp-server user	Defines a user who can access the SNMP engine.
snmp-server view	Defines a SNMPv2 Management Information Base (MIB) view.

snmp-server location

To set the Simple Network Management Protocol(SNMP) system location string, use the **snmp-server location** command in global configuration mode. To remove the location string, use the **no** form of this command.

snmp-server location *line*

no snmp-server location

Syntax Description

line	String that describes the physical location of this node.

Defaults

No system location string is set.

Command Modes

Global configuration (config) mode.

Usage Guidelines

The system location string is the value stored in the MIB-II system group system location object. You can see the system location string with the **show snmp** command.

Examples

The following example shows how to configure a system location string:

```
ServiceEngine(config)# snmp-server location Building 3/Room 214
```

Related Commands

Command	Description
show snmp	Displays the SNMP parameters.
snmp-server community	Configures the community access string to permit access to the SNMP.
snmp-server contact	Sets the system server contact string.
snmp-server enable traps	Enables the Service Engine (SE) to send SNMP traps.
snmp-server group	Defines a user security model group.
snmp-server host	Specifies the hosts to receive SNMP traps.
snmp-server notify inform	Configures the SNMP notify inform request.
snmp-server user	Defines a user who can access the SNMP engine.
snmp-server view	Defines a SNMPv2 Management Information Base (MIB) view.

snmp-server notify inform

To configure the Simple Network Management Protocol (SNMP) notify inform request, use the **snmp-server notify inform** command in global configuration mode. To return the setting to the default value, use the **no** form of this command.

snmp-server notify inform

no snmp-server notify inform

Syntax Description

This command has no arguments or keywords.

Defaults

If you do not enter the **snmp-server notify inform** command, the default is an SNMP trap request.

Command Modes

Global configuration (config) mode.

Usage Guidelines

The **snmp-server host** command specifies which hosts receive informs. The **snmp-server enable traps** command globally enables the production mechanism for the specified notifications (traps and informs).

For a host to receive an inform, enable the inform globally by entering the **snmp-server notify inform** command.

The SNMP inform requests feature allows SEs to send inform requests to SNMP managers. SEs can send notifications to SNMP managers when particular events occur. For example, an agent SE might send a message to a manager when the agent SE experiences an error condition.

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send any acknowledgment when it receives a trap. The sender cannot determine if the trap was received. However, an SNMP manager that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the manager does not receive an inform request, it does not send a response. If the sender never receives a response, the inform request can be sent again. Informs are more likely to reach their intended destination.

Because they are more reliable, informs consume more resources in the SE and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in the memory until a response is received or the request times out. Also, traps are sent only once, while an inform may be retried several times. The retries increase traffic and contribute to a higher overhead on the network. Traps and inform requests provide a trade-off between reliability and resources.

Tip If it is important that the SNMP manager receives every notification, then you should use inform requests in your network. If you are concerned about traffic on your network or about the memory in the SE and you do not need to receive every notification, then you should use traps in your network.

Examples

The following example shows how to configure the SNMP notify inform request on the SE:

```
ServiceEngine(config)# snmp-server notify inform
```

Related Commands

Command	Description
show snmp	Displays the SNMP parameters.
snmp-server community	Configures the community access string to permit access to the SNMP.
snmp-server contact	Sets the system server contact string.
snmp-server enable traps	Enables the Service Engine (SE) to send SNMP traps.
snmp-server group	Defines a user security model group.
snmp-server host	Specifies the hosts to receive SNMP traps.
snmp-server location	Sets the SNMP system location string.
snmp-server user	Defines a user who can access the SNMP engine.
snmp-server view	Defines a SNMPv2 Management Information Base (MIB) view.

snmp-server user

To define a user who can access the Simple Network Management Protocol (SNMP) server, use the **snmp-server user** command in global configuration mode. To remove access, use the **no** form of this command.

snmp-server user *name group* [**auth** {**md5** *password* [**priv** *password*] | **sha** *password* [**priv** *password*]} | **remote** *octet_string* [**auth** {**md5** *password* [**priv** *password*] | **sha** *password* [**priv** *password*]}]]

no snmp-server user *name group* [**auth** {**md5** *password* | **sha** *password*} [**priv** *password*] | **remote** *octetstring* [**auth** {**md5** *password* | **sha** *password*} [**priv** *password*]]]

Syntax Description

name	Name of the SNMP user. Use letters, numbers, dashes, and underscores, but no blanks. This is the name of the user on the SNMP host who wants to communicate with the SNMP agent on the SE. You can enter a maximum of 64 characters.
group	Name of the group to which the SNMP user belongs. You can enter a maximum of 64 characters.
auth	(Optional) Configures user authentication parameters.
md5	Configures the Hashed-Based Message Authentication Code Message Digest 5 (HMAC MD5) authentication algorithm.
password	HMAC MD5 user authentication password.
priv	(Optional) Configures authentication parameters for the packet.
password	HMAC MD5 user private password. You can enter a maximum of 256 characters.
sha	Configures the HMAC Secure Hash Algorithm (SHA) authentication algorithm.
password	HMAC SHA authentication password. You can enter a maximum of 256 characters.
remote	(Optional) Specifies the engine identity of the remote SNMP entity to which the user belongs.
octet_string	Globally unique identifier for a remote SNMP entity (for example, the SNMP network management station) for at least one of the SNMP users.

Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

The maximum number of SNMP users that can be created is 10. Follow these guidelines when defining SNMP users for SEs:

- If SNMPv3 is going to be used for SNMP requests, define at least one SNMPv3 user account on the SE for the SE to be accessed through SNMP.
- Group defined with the SNMPv1 or SNMPv2c security model should not be associated with SNMP users; they should only be associated with the community strings.

Tip To send an SNMPv3 inform message, you must configure at least one SNMPv3 user with a remote SNMP ID option on the SE. The SNMP ID is entered in octet string form. For example, if the IP address of a remote SNMP entity is 192.147.142.129, then the octet string would be 00:00:63:00:00:00:a1:c0:93:8e:81.

Examples

The following example shows that an SNMPv3 user account is created on the SE. The SNMPv3 user is named acme and belongs to the group named admin. Because this SNMP user account has been set up with no authentication password, the SNMP agent on the SE does not perform authentication on SNMP requests from this user.

```
ServiceEngine(config)#  snmp-server user acme admin
```

Related Commands

Command	Description
show snmp	Displays the SNMP parameters.
snmp-server community	Configures the community access string to permit access to the SNMP.
snmp-server contact	Sets the system server contact string.
snmp-server enable traps	Enables the Service Engine (SE) to send SNMP traps.
snmp-server group	Defines a user security model group.
snmp-server host	Specifies the hosts to receive SNMP traps.
snmp-server location	Sets the SNMP system location string.
snmp-server notify inform	Configures the SNMP notify inform request.
snmp-server view	Defines a SNMPv2 Management Information Base (MIB) view.

snmp-server view

To define a Simple Network Management Protocol Version 2 (SNMPv2) Management Information Base (MIB) view, use the **snmp-server view** command in global configuration mode. To undefine the MIB view, use the **no** form of this command.

snmp-server view *view_name MIB_family* {**excluded** | **included**}

no snmp-server view *view_name MIB_family* {**excluded** | **included**}

Syntax Description

view_name	Name of this family of view subtrees. You can enter a maximum of 64 characters.
MIB_family	An object identifier that identifies a subtree of the MIB. You can enter a maximum of 64 characters.
excluded	Excludes the MIB family from the view.
included	Includes the MIB family from the view.

Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

An *SNMP view* is a mapping between SNMP objects and the access rights available for those objects. An object can have different access rights in each view. Access rights indicate whether the object is accessible by either a community string or a user. The **snmp-server view** command is used with the **snmp-server group** to limit the read-write access of MIB trees based on the group. Because the group can be associated with the SNMP community string or users, using the **snmp-server view** command extends the limit to users and community strings. If the view is not configured, read-write access to the community string applies to the MIB tree and all users (SNMPv3).

The maximum number of views that can be created is 10. You can configure the SNMP view settings only if you have previously configured the SNMP server settings.

To remove a view record, use the **no snmp-server view** command.

You can enter the **snmp-server view** command multiple times for the same view record. Later lines take precedence when an object identifier is included in two or more lines.

Note When configuring an SNMP View with Excluded, the specified MIB that is excluded is not accessible for the community associated with the group that has that view.

Examples

The following example shows how to configure the view name, family name, and view type:

```
ServiceEngine(config)# snmp-server view contentview ciscoServiceEngineMIB included
```

The following example creates a view that includes all objects in the MIB-II system group and all objects in the Cisco enterprise MIB:

```
ServiceEngine(config)# snmp-server view phred system included
ServiceEngine(config)# snmp-server view phred cisco included
```

The following example shows how to create a view that includes all objects in the MIB-II system group except for sysServices (System 7) in the MIB-II interfaces group:

```
ServiceEngine(config)# snmp-server view agon system included
ServiceEngine(config)# snmp-server view agon system.7 excluded
```

Related Commands

Command	Description
show snmp	Displays the SNMP parameters.
snmp-server community	Configures the community access string to permit access to the SNMP.
snmp-server contact	Sets the system server contact string.
snmp-server enable traps	Enables the Service Engine (SE) to send SNMP traps.
snmp-server group	Defines a user security model group.
snmp-server host	Specifies the hosts to receive SNMP traps.
snmp-server location	Sets the SNMP system location string.
snmp-server notify inform	Configures the SNMP notify inform request.
snmp-server user	Defines a user who can access the SNMP engine.

SS

To dump socket statistics, use the **ss** command in EXEC configuration mode.

ss *line*

Syntax Description

line	ss connection information, -h to get help.

Command Defaults

None

Command Modes

EXEC configuration.

Usage Guidelines

The **ss** utility is used to dump socket statistics. It shows information similar to the **netstat** command and displays more TCP information than other tools.

When specifying the options and filters, you can use the short form of the option (a single dash followed by a character) or the long form of the option (two dashes followed by the whole word). To view the list of options and filters, enter **ss -h** (or **ss --help**) and the list of options and filters are displayed along with descriptions.

```
ServiceEngine# ss -h
Usage: ss [OPTIONS]
       ss [OPTIONS] [FILTER]
   -h, --help           this message
   -V, --version        output version information
   -n, --numeric        does not resolve service names
   -r, --resolve        resolve host names
   -a, --all            display all sockets
   -l, --listening      display listening sockets
   -o, --options        show timer information
   -e, --extended       show detailed socket information
   -m, --memory         show socket memory usage
   -p, --processes      show process using socket
   -i, --info           show internal TCP information
   -s, --summary        show socket usage summary

   -4, --ipv4           display only IP version 4 sockets
   -6, --ipv6           display only IP version 6 sockets
   -0, --packet         display PACKET sockets
   -t, --tcp            display only TCP sockets
   -u, --udp            display only UDP sockets
   -d, --dccp           display only DCCP sockets
   -w, --raw            display only RAW sockets
   -x, --unix           display only Unix domain sockets
   -7, --filter display when tcp rqueue threshold meet
   -8, --filter display when tcp wqueue threshold meet
   -9, --filter display when tcp retransmit threshold meet
   -W, --filter display only window scale disable
   -B, --background display output in new format
   -L, --no_loop_back   display without loopback interface
   -S, --basic_output  display basic information
   -f, --family=FAMILY display sockets of type FAMILY
```

```
-A, --query=QUERY
    QUERY := {all | inet | tcp | udp | raw | unix | packet | netlink}[,QUERY]

-F, --filter=FILE   read filter information from FILE
    FILTER := [state TCP-STATE] [EXPRESSION]
```

With the **-A** query option, you list the identifiers (all, inet, tcp, udp, and so on) of the socket tables you want displayed, separated by commas.

With the -F filter option, you can filter by TCP state, or using a boolean expression you can filter by IP addresses and ports.

The default output does not resolve host addresses (IP addresses) and does resolve service names (usually stored in local files). To resolve host addresses, use the **-r** option. To suppress resolution of service names, use the **-n** option.

Examples

The following command shows how to display all TCP sockets:

```
ServiceEngine# ss -t -a
```

The following command shows how to display all UDP sockets:

```
ServiceEngine# ss -u -a
```

The following command shows how to display all established SSH connections and display the timer information:

```
ServiceEngine# ss -o state established '(dport = :ssh or sport = :ssh)'
```

The following command shows how to display all established HTTP connections and display the timer information:

```
ServiceEngine# ss -o state established '(dport = :http or sport = :http)'
```

Related Commands

Command	Description
gulp	Captures lossless gigabit packets and writes them to disk.
netmon	Displays the transmit and receive activity on an interface.
netstatr	Displays the rate of change of netstat statistics.
tcpmon	Searches all TCP connections.

ssh-key-generate

To generate the SSH host key, use the **ssh-key-generate** command in global configuration mode. To disable the SSH key, use the **no** form of this command.

ssh-key-generate [**key-length** *num*]

no ssh-key-generate [**key-length** *num*]

Syntax Description

key-length	Configures the length of SSH key.
num	Specifies the number of bits in the SSH key to create.

Defaults

key-length *bits*: 2048

Command Modes

Global configuration (config) mode.

Usage Guidelines

SSH enables login access to the SE through a secure and encrypted channel. SSH consists of a server and a client program. Like Telnet, you can use the client program to remotely log on to a machine that is running the SSH server, but unlike Telnet, messages transported between the client and the server are encrypted. The functionality of SSH includes user authentication, message encryption, and message authentication.

When you enable the SSH server, the Secure File Transfer Protocol (SFTP) server is also enabled. The SFTP is a file transfer program that provides a secure and authenticated method for transferring files between VDS-OS devices and other workstations or clients.

Note SFTP is the standard file transfer protocol introduced in SSH Version 2. The SFTP client functionality is provided as part of the SSH component. If you use SSH Version 1 on the SE, SFTP support is not available.

Examples

The following example shows how to generate an SSH host key on an SE:

```
ServiceEngine(config)# ssh-key-generate key-length 2048
```

The following example disables the ssh host key:

```
ServiceEngine(config)# no ssh-key-generate key-length 2048
```

Related Commands

Command	Description
show ssh	Displays the SSH status and configuration.

sshd

To enable the Secure Shell (SSH) daemon, use the **sshd** command in global configuration mode. To disable SSH, use the **no** form of this command.

sshd {**enable** | **timeout** *seconds* | **version** {**1** | **2**}}

no sshd {**enable** | **password-guesses** | **timeout** | **version** {**1** | **2**}}

Syntax Description

enable	Enables the SSH feature.
timeout	Configures the number of seconds for which an SSH session is active during the negotiation (authentication) phase between the client and the server before it times out. **Note** If you have established an SSH connection to the SE but have not entered the username when prompted at the login prompt, the connection is terminated by the SE even after successful login if the grace period expires.
seconds	SSH login grace time value, in seconds. The range is from 1 to 99999. The default is 300.
version	Configures the SSH version to be supported on the SE.
1	Specifies that SSH Version 1 is supported on the SE.
2	Specifies that SSH Version 2 is supported on the SE.

Defaults

timeout *seconds*: 300

version: Both SSH Version 1 and 2 are enabled.

Command Modes

Global configuration (config) mode.

Usage Guidelines

SSH enables login access to the SE through a secure and encrypted channel. SSH consists of a server and a client program. Like Telnet, you can use the client program to remotely log on to a machine that is running the SSH server, but unlike Telnet, messages transported between the client and the server are encrypted. The functionality of SSH includes user authentication, message encryption, and message authentication.

When you enable the SSH server, the Secure File Transfer Protocol (SFTP) server is also enabled. The SFTP is a file transfer program that provides a secure and authenticated method for transferring files between VDS-OS devices and other workstations or clients.

Note SFTP is the standard file transfer protocol introduced in SSH Version 2. The SFTP client functionality is provided as part of the SSH component. If you use SSH Version 1 on the SE, SFTP support is not available.

The **sshd version** command in global configuration mode allows you to enable support for either SSH Version 1 or SSH Version 2. When you enable SSH using the **sshd enable** command in global configuration mode, the VDS-OS software enables support for both SSH Version 1 and SSH Version 2 on the SE. If you want the SE to support only one version of SSH (for example SSH Version 2), disable the other version (in this example, SSH Version 1) by using the **no sshd version 1** command.

When support for both SSH Version 1 and SSH Version 2 are enabled in the SE, the **show running-config** command output does not display any sshd configuration. If you have disabled the support for one version of SSH, the **show running-config** command output contains the following line:

```
no sshd version version_number
```

Note You cannot disable both SSH versions in an SE. Use the **no sshd enable** command in global configuration mode to disable SSH on the SE.

Examples

The following example shows how to enable the SSH daemon and configure the number of allowable password guesses and timeout for the SE:

```
ServiceEngine(config)# sshd enable
ServiceEngine(config)# sshd password-guesses 4
ServiceEngine(config)# sshd timeout 20
```

The following example disables the support for SSH Version 1 in the SE:

```
ServiceEngine(config)# no sshd version 1
```

Related Commands

Command	Description
show ssh	Displays the SSH status and configuration.

streaming-interface

To configure the streaming interface, use the **streaming-interface** command in global configuration mode. To remove a streaming interface, use the **no** form of this command.

streaming-interface {**GigabitEthernet** *num* | **PortChannel** *num* | **Standby** *num*}

Syntax Description

GigabitEthernet	Selects a Gigabit Ethernet interface as streaming interface.
num	Gigabit Ethernet slot (the range is 1 to 14) and port (the range is 0 to 0).
PortChannel	Selects a port channel interface as streaming interface.
num	Port channel port.
Standby	Selects a standby group as streaming interface.
num	Standby group number.

Command Default

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

When upgrading from a previous software release, the primary interface is converted to a streaming interface by the upgrade process. When configuring new delivery traffic interfaces, either because of a new installation or because of removing existing configuration, use the **streaming-interface** command.

Examples

The following example shows how to configure port channel 1 as the streaming interface:

```
ServiceEngine# streaming-interface portChannel 1

ServiceEngine#
```

sysreport

To save the sysreport to a user-specified file, use the **sysreport** privilege command in EXEC configuration mode.

sysreport {**authentication** [**date-range** *start_date end_date* | *filename*] | **cms** [**date-range** *start_date end_date* | *filename*] | **dns** | **ftp** | **http** | **icap**}

Syntax Description

authentication	Generates sysreport information related to HTTP authentication.
cms	Generates sysreport information related to Centralized Management System (CMS).
dns	Generates sysreport information related to Domain Name Server (DNS).
ftp	Generates sysreport information related to File Transfer Protocol (FTP).
http	Generates sysreport information related to HTTP.
icap	Generates sysreport information related to Internet Content Adaptation Protocol (ICAP).

Defaults

None

Command Modes

Privilege EXEC configuration mode.

Examples

The following example saves the sysreport for authentication to user-specified file **xxx.tar.gz**:

```
ServiceEngine# sysreport authentication date-range 2009/05/07 2009/05/11 xxx.tar.gz
The sysreport has been saved onto file xxx.tar.gz in local1
```

tacacs

To configure Terminal Access Controller Access Control System Plus (TACACS+) server parameters, use the **tacacs** command in global configuration mode. To disable individual options, use the **no** form of this command.

tacacs {**host** {*hostname* | *ip_address*} [**primary**] | **key** *keyword* | **password ascii** | **retransmit** *retries* | **timeout** *seconds*}

no tacacs {**host** {*hostname* | *ip_address*} [**primary**] | **key** | **password ascii** | **retransmit** | **timeout**}

Syntax Description

host	Sets a server address.
hostname	Hostname of the TACACS+ server.
ip_address	IP address of the TACACS+ server.
primary	(Optional) Sets the server as the primary server.
key	Sets the security word.
keyword	Keyword. An empty string is the default.
password ascii	Specifies ASCII as the TACACS+ password type.
retransmit	Sets the number of times that requests are retransmitted to a server.
retries	Number of retry attempts allowed. The range is from 1 to 3. The default is 2.
timeout	Sets the number of seconds to wait before a request to a server is timed out.
seconds	Timeout, in seconds. The range is from 1 to 20. The default is 5.

Defaults

keyword: none (empty string)

timeout *seconds*: 5

retransmit *retries*: 2

password ascii: PAP

Command Modes

Global configuration (config) mode.

Usage Guidelines

Using the **tacacs** command, configure the TACACS+ key, the number of retransmits, the server hostname or IP address, and the timeout.

Execute the following two commands to enable user authentication with a TACACS+ server:

```
ServiceEngine(config)# authentication login tacacs enable
ServiceEngine(config)# authentication configuration tacacs enable
```

HTTP request authentication is independent of user authentication options and must be disabled with the following separate commands:

```
ServiceEngine(config)# no authentication login tacacs enable
ServiceEngine(config)# no authentication configuration tacacs enable
```

The Users GUI page or the **username** command in global configuration provide a way to add, delete, or modify usernames, passwords, and access privileges in the local database. The TACACS+ remote database can also be used to maintain login and configuration privileges for administrative users. The **tacacs host** command or the TACACS+ Service Engine GUI page allows you to configure the network parameters required to access the remote database.

One primary and two backup TACACS+ servers can be configured; authentication is attempted on the primary server first and then on the others in the order in which they were configured. The primary server is the first server configured unless another server is explicitly specified as primary with the **tacacs host** *hostname* **primary** command.

Use the **tacacs key** command to specify the TACACS+ key that is used to encrypt the packets sent to the server. This key must be the same as the one specified on the server daemon. The maximum number of characters in the 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.

The **tacacs timeout** is the number of seconds that the Service Engine waits before declaring a timeout on a request to a particular TACACS+ server. The range is from 1 to 20 seconds with 5 seconds as the default. The number of times that the Service Engine repeats a retry-timeout cycle before trying the next TACACS+ server is specified by the **tacacs retransmit** command. The default is two retry attempts.

Three unsuccessful login attempts are permitted. TACACS+ logins may appear to take more time than local logins depending on the number of TACACS+ servers and the configured timeout and retry values.

Use the **tacacs password ascii** command to specify the TACACS+ password type as ASCII. The default password type is Password Authentication Protocol (PAP). In earlier releases, the password type was not configurable. When users needed to log in to a Service Engine, a TACACS+ client sent the password information in PAP format to a TACACS+ server. However, TACACS+ servers that were configured for router management required the passwords to be in ASCII cleartext format instead of PAP format to authenticate users logging in to the Service Engine. The password type to authenticate user information to ASCII was configurable from the CLI.

Note When the **no tacacs password ascii** command is used to disable the ASCII password type, the password type is once again reset to PAP.

The TACACS+ client can send different requests to the server for user authentication. The client can send a TACACS+ request with the PAP password type. In this scenario, the authentication packet includes both the username and the user's password. The server must have an appropriately configured user's account.

Alternatively, the client can send a TACACS+ request with the ASCII password type as another option. In this scenario, the authentication packet includes the username only and waits for the server response. Once the server confirms that the user's account exists, the client sends another Continue request with the user's password. The Authentication Server must have an appropriately configured user's account to support either type of password.

Examples

The following example shows how to configure the key used in encrypting packets:

```
ServiceEngine(config)# tacacs key human789
```

The following example shows how to configure the host named spearhead as the primary TACACS+ server:

```
ServiceEngine(config)# tacacs host spearhead primary
```

The following example shows how to set the timeout interval for the Terminal Access Controller Access Control System Plus (TACACS+) server:

```
ServiceEngine(config)# tacacs timeout 10
```

The following example shows how to set the number of times that authentication requests are retried (retransmitted) after a timeout:

```
ServiceEngine(config)# tacacs retransmit 5
```

The following example shows the password type to be PAP by default:

```
ServiceEngine# show tacacs
    Login Authentication for Console/Telnet Session: enabled (secondary)
    Configuration Authentication for Console/Telnet Session: enabled (secondary)

    TACACS+ Configuration:
    ---------------------
    TACACS+ Authentication is off
    Key        = *****
    Timeout    = 5
    Retransmit = 2
    Password type: pap

    Server                         Status
    ----------------------------   ------
    10.107.192.148                primary
    10.107.192.168
    10.77.140.77
ServiceEngine#
```

However, you can configure the password type to be ASCII using the **tacacs password ascii** command. You can then verify the changes using the **show tacacs** command as follows:

```
ServiceEngine(config)# tacacs password ascii
ServiceEngine(config)# exit
ServiceEngine# show tacacs
    Login Authentication for Console/Telnet Session: enabled (secondary)
    Configuration Authentication for Console/Telnet Session: enabled (secondary)

    TACACS+ Configuration:
    ---------------------
    TACACS+ Authentication is off
    Key        = *****
    Timeout    = 5
    Retransmit = 2
    Password type: ascii

    Server                         Status
    ----------------------------   ------
    10.107.192.148                primary
    10.107.192.168
    10.77.140.77
```

Related Commands

Command	Description
show authentication	Displays the authentication configuration.
show statistics tacacs	Displays the Service Engine TACACS+ authentication and authorization statistics.
show tacacs	Displays TACACS+ authentication protocol configuration information.

tcpdump

To dump the network traffic, use the **tcpdump** command in EXEC configuration mode.

tcpdump [*LINE*]

Syntax Description

LINE	(Optional) Dump options.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use the **tcpdump** command to gather a sniffer trace on the SE, SR, or VOSM for troubleshooting when asked to gather the data by the Cisco Technical Support. This utility is very similar to the Linux or UNIX **tcpdump** command.

The **tcpdump** command allows an administrator (must be an admin user) to capture packets from the Ethernet. On the SE 500 series, the interface names are GigabitEthernet 1/0 and GigabitEthernet 2/0. On all VDS-OS platforms, we recommend that you specify a path/filename in the local1 directory.

You can do a straight packet header dump to the screen by entering the **tcpdump** command. Press **Ctrl-C** to stop the dump.

The **tcpdump** command has the following options:

- **-w** <*filename*>—Writes the raw packet capture output to a file.
- **-s** <*count*>—Captures the first <*count*> bytes of each packet.
- **-i** <*interface*>—Allows you to specify a specific interface to use for capturing the packets.
- **-c** <*count*>—Limits the capture to <*count*> packets.

The following example captures the first 1500 bytes of the next 10,000 packets from interface Ethernet 0 and puts the output in a file named dump.pcap in the local1 directory on the SE:

```
ServiceEngine# tcpdump -w /local1/dump.pcap -i GigabitEthernet 1/0 -s 1500 -c 10000
```

When you specify the **-s** option, it sets the packet snap length. The default value captures only 64 bytes, and this default setting saves only packet headers into the capture file. For troubleshooting of redirected packets or higher level traffic (HTTP, authentication, and so on), copy the complete packets.

After the TCP dump has been collected, you need to move the file from the SE to a PC so that the file can be viewed by a sniffer decoder.

```
ftp <ip address of the SE>

!--- Log in using the admin username and password.

    cd local1
    bin
    hash
```

```
     get <name of the file>

!--- Using the above example, it would be dump.pcap.

     bye
```

We recommend that you use Ethereal as the software application for reading the TCP dump. With Ethereal, you can decode packets that are encapsulated into a generic routing encapsulation (GRE) tunnel. See the Ethereal website for further information.

Note In most cases, redirected packets captured by the tcpdump facility with the VDS-OS CLI differ from the data received on the interface. The destination IP address and TCP port number are modified to reflect the device IP address and the port number 8999.

Examples

The following example shows how to dump the TCP network traffic:

```
ServiceEngine# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on GigabitEthernet 1/0, link-type EN10MB (Ethernet), capture size 68 bytes
12:45:43.017677 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P
3342832089:3342832201(112) ack 1248615673 win 15232
12:45:43.018950 IP 172.19.226.63 > ServiceEngine.cisco.com: icmp 36: 172.19.226.63 udp
port 2048 unreachable
12:45:43.019327 IP ServiceEngine.cisco.com.10015 > dns-sj2.cisco.com.domain: 49828+ [  |
domain ]
12:45:43.021158 IP dns-sj2.cisco.com.domain > ServiceEngine.cisco.com.10015: 49828
NXDomain* [  | domain ]
12:45:43.021942 IP ServiceEngine.cisco.com.10015 > dns-sj2.cisco.com.domain: 49829+ [  |
domain ]
12:45:43.023799 IP dns-sj2.cisco.com.domain > ServiceEngine.cisco.com.10015: 49829
NXDomain* [  | domain ]
12:45:43.024240 IP ServiceEngine.cisco.com.10015 > dns-sj2.cisco.com.domain: 49830+ [  |
domain ]
12:45:43.026164 IP dns-sj2.cisco.com.domain > ServiceEngine.cisco.com.10015: 49830* [  |
domain ]
12:45:42.702891 802.1d config TOP_CHANGE 8000.00:03:9f:f1:10:63.8042 root
8000.00:01:43:9a:c8:63 pathcost 26 age 3 max 20 hello 2 fdelay 15
12:45:42.831404 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 112 win 64351
12:45:42.831490 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: . 112:1444(1332) ack 1
win 15232
12:45:42.831504 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 1444:1568(124) ack 1
win 15232
12:45:42.831741 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 1568:1696(128) ack 1
win 15232
12:45:43.046176 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 1568 win 65535
12:45:43.046248 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 1696:2128(432) ack 1
win 15232
12:45:43.046469 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 2128:2256(128) ack 1
win 15232
12:45:43.046616 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 2256:2400(144) ack 1
win 15232
12:45:43.107700 802.1d config TOP_CHANGE 8000.00:03:9f:f1:10:63.8042 root
8000.00:01:43:9a:c8:63 pathcost 26 age 3 max 20 hello 2 fdelay 15
12:45:43.199710 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 1696 win 65407
12:45:43.199784 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 2400:2864(464) ack 1
win 15232
12:45:43.199998 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 2864:2992(128) ack 1
win 15232
```

```
12:45:43.259968 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 2400 win 64703
12:45:43.260064 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 2992:3280(288) ack 1
win 15232
12:45:43.260335 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 3280:3408(128) ack 1
win 15232
12:45:43.260482 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 3408:3552(144) ack 1
win 15232
12:45:43.260621 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 3552:3696(144) ack 1
win 15232
12:45:43.413320 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 2992 win 65535
12:45:43.413389 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 3696:3984(288) ack 1
win 15232
12:45:43.413597 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 3984:4112(128) ack 1
win 15232
12:45:43.413741 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 4112:4256(144) ack 1
win 15232
12:45:43.473601 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 3552 win 64975
12:45:43.473659 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 4256:4544(288) ack 1
win 15232
12:45:43.473853 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 4544:4672(128) ack 1
win 15232
12:45:43.473994 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 4672:4816(144) ack 1
win 15232
12:45:43.474132 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 4816:4960(144) ack 1
win 15232
12:45:43.484117 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: P 1:81(80) ack 3696
win 64831
12:45:43.484167 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 4960:5248(288) ack
81 win 15232
12:45:43.484424 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 5248:5392(144) ack
81 win 15232
12:45:43.627125 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 4112 win 64415
12:45:43.627204 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 5392:5680(288) ack
81 win 15232
12:45:43.627439 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 5680:5808(128) ack
81 win 15232
12:45:43.627586 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 5808:5952(144) ack
81 win 15232
12:45:43.688261 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 4544 win 65535
12:45:43.688316 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 5952:6240(288) ack
81 win 15232
12:45:43.688495 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 6240:6368(128) ack
81 win 15232
12:45:43.688638 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 6368:6512(144) ack
81 win 15232
12:45:43.689012 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 4960 win 65119
12:45:43.689046 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 6512:6800(288) ack
81 win 15232
12:45:43.689170 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 6800:6928(128) ack
81 win 15232
12:45:43.689309 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 6928:7072(144) ack
81 win 15232
12:45:43.689447 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 7072:7216(144) ack
81 win 15232
12:45:43.698391 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 5392 win 64687
12:45:43.698437 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 7216:7504(288) ack
81 win 15232
12:45:43.698599 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 7504:7632(128) ack
81 win 15232
12:45:43.698740 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 7632:7776(144) ack
81 win 15232
12:45:43.840558 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 5808 win 64271
12:45:43.840622 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 7776:8064(288) ack
81 win 15232
```

```
12:45:43.840819 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 8064:8192(128) ack
81 win 15232
12:45:43.840962 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 8192:8336(144) ack
81 win 15232
12:45:43.901868 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 6368 win 65535
12:45:43.901938 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 8336:8624(288) ack
81 win 15232
12:45:43.901887 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 6928 win 64975
12:45:43.901910 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 7216 win 64687
12:45:43.902137 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 8624:8752(128) ack
81 win 15232
12:45:43.902281 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 8752:8896(144) ack
81 win 15232
12:45:43.902414 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 8896:9024(128) ack
81 win 15232
12:45:43.902547 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 9024:9152(128) ack
81 win 15232
12:45:43.902687 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 9152:9296(144) ack
81 win 15232
12:45:43.902826 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 9296:9440(144) ack
81 win 15232
12:45:43.902965 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 9440:9584(144) ack
81 win 15232
12:45:43.903104 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 9584:9728(144) ack
81 win 15232
12:45:43.922413 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 7632 win 64271
12:45:43.922459 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 9728:10304(576) ack
81 win 15232
12:45:43.922622 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 10304:10432(128) ack
81 win 15232
12:45:43.922764 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 10432:10576(144) ack
81 win 15232
12:45:44.053872 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 8192 win 65535
12:45:44.053972 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 10576:10864(288) ack
81 win 15232
12:45:44.054308 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 10864:11104(240) ack
81 win 15232
12:45:44.054453 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 11104:11248(144) ack
81 win 15232
12:45:44.054596 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 11248:11392(144) ack
81 win 15232
12:45:44.111702 802.1d config TOP_CHANGE 8000.00:03:9f:f1:10:63.8042 root
8000.00:01:43:9a:c8:63 pathcost 26 age 3 max 20 hello 2 fdelay 15
12:45:44.114626 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 8752 win 64975
12:45:44.114712 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 11392:11712(320) ack
81 win 15232
12:45:44.115219 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 11712:11952(240) ack
81 win 15232
12:45:44.115381 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 11952:12096(144) ack
81 win 15232
12:45:44.115426 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 9152 win 64575
12:45:44.115617 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 12096:12336(240) ack
81 win 15232
12:45:44.115760 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 12336:12480(144) ack
81 win 15232
12:45:44.115904 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 12480:12624(144) ack
81 win 15232
12:45:44.116045 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 12624:12768(144) ack
81 win 15232
12:45:44.116094 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 9440 win 64287
12:45:44.116114 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 9728 win 65535
12:45:44.116332 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 12768:13088(320) ack
81 win 15232
```

```
12:45:44.116473 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 13088:13232(144) ack
81 win 15232
12:45:44.116614 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 13232:13376(144) ack
81 win 15232
12:45:44.116755 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 13376:13520(144) ack
81 win 15232
12:45:44.116895 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 13520:13664(144) ack
81 win 15232
12:45:44.135947 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 10432 win 64831
12:45:44.135996 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 13664:13808(144) ack
81 win 15232
12:45:44.136223 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 13808:14048(240) ack
81 win 15232
12:45:44.136366 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 14048:14192(144) ack
81 win 15232
12:45:44.144104 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: P 81:161(80) ack 10576
win 64687

102 packets captured
105 packets received by filter
0 packets dropped by kernel
```

The following example shows how to dump the TCP network traffic and redirect it to a file named test:

```
ServiceEngine# tcpdump port 8080 -w test
tcpdump: listening on GigabitEthernet 1/0, link-type EN10MB (Ethernet), capture size 68
bytes
216 packets captured
216 packets received by filter
0 packets dropped by kernel
```

tcpdumpx

To dump the network traffic with the tcpdump extension for a multi-interface capture, use the **tcpdumpx** command in EXEC configuration mode.

tcpdumpx [*LINE*]

Syntax Description

LINE	(Optional) Dump options, -h to get help.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **tcpdumpx** command enables tcpdump to capture multiple interfaces in separate files. Each member interface of a PortChannel can be captured in a separate file. For example, if eth2, eth3, eth4 and eth5 are members of PortChannel 1 (bond0), they can be captured in different files.

Current: issue "tcpdump -i" for each PortChannel member in a different shell at the same time.

Implemented: New flag (-j), not used by tcpdump, under tcpdumpx handles this:

```
tcpdumpx -j PortChannel 1 -w filename.cap
```

This command internally expands to capture each physical interface's dump in an individual file:

```
tcpdump -i eth2 -w filename.eth2.cap
tcpdump -i eth3 -w filename.eth3.cap
tcpdump -i eth4 -w filename.eth4.cap
tcpdump -i eth5 -w filename.eth5.cap
```

If eth2 and eth3 need to be captured, use "--" as a command separator to separate the two tcpdump instances:

```
tcpdumpx -i eth2 -w filename.cap -k -m -- -i eth3 -w filename2.cap -c -k -- … --
```

This command internally expands to:

```
tcpdump -i eth2 -w filename.cap
tcpdump -i eth3 -w filename.cap
```

Other examples:

```
tcpdumpx -j PortChannel 1 -w filename.cap -- -j PortChannel 2 -w filename2.cap
tcpdumpx -i eth2 -w filename.cap -- -i eth3 -w filename2.cap -- j PortChannel 1 -w
filename3.cap
```

This is documented in tcpdumpx help "tcpdumpx -h":

```
tcpdump                   Dump traffic on a network
tcpdumpx                 tcpdump extension for multi-interface capture
tcpdumpx -h
tcpdumpx - tcpdump extension for multiple interface capture
[WARNING] This program consumes HIGH CPU & memory and impacts system performance

Usage: tcpdumpx [-w filename] [-j PortChannel X] [--] [all tcpdump options]
```

```
[-w filename]          Required. Write tcpdump output to filename
[-j PortChannel X]     Capture each PortChannel slave to file:
                       "filename" --> "filenameslavename"
                       "filename.xxx"   --> "filename.slavename.xxx"
[--]                   Interface separator. Capture Multiple Interfaces by:
                       tcpdumpx -i eth0 -w eth0 -- -i eth2 -w eth2 -- . . . -- . .
                       tcpdumpx -i eth0 -w eth0 -- -j PortChannel 1 -w pc
                       tcpdumpx -j PortChannel 1 -w pc1 -- -j PortChannel 2
                       -w pc2
[all tcpdump options] Specify any tcpdump options
                       Please use "tcpdump -h" to get tcpdump help options
[-h(elp)]              Print this help
```

Examples

The following example shows how to dump the TCP network traffic with a tcpdump extension for multi-interface capture:

```
ServiceEngine# tcpdumpx
```

tcpmon

To search all TCP connections, use the **tcpmon** command in EXEC configuration mode.

tcpmon *line*

Syntax Description

line	Shows TCP connection information, -h to get help.

Command Defaults

None

Command Modes

EXEC configuration.

Usage Guidelines

The **tcpmon** utility is a script that constantly calls the ss utility at specified intervals. The **tcpmon** utility searches all TCP connections every 30 seconds and displays information about any socket that meets the search criteria. To view the list of options, enter **tcpmon -h**.

Table 2-69 describes the tcpmon output fields.

Table 2-69 tcpmon Output Fields

Field	Description
State	One of the following TCP connection states: ESTAB, SYN-SENT, SYN-RECV, FIN-WAIT-1, FIN-WAIT-2, TIME-WAIT, CLOSE-WAIT, LAST-ACK, LISTEN, and CLOSING.
Recv-Q	Number of bytes in the receiving queue.
Send-Q	Number of bytes in the sending queue.
Local Address: Port	Source address and port.
Peer Address: Port	Destination address and port.
Rtt/var	Average round-trip time (in seconds) and the deviation.
Send	Current sending rate (in Mbps).
Retrans	Number of retransmit timeouts.

Examples

The following command sets the polling cycle to 30 seconds and the receive-queue threshold to 100:

```
ServiceEngine# tcpmon -R 100 30
```

The following command sets the polling cycle to 30 seconds and displays only the sockets with window scaling disabled:

```
ServiceEngine# tcpmon -N 30
```

The following example shows the output for the **tcpmon** utility:

```
State   Recv-Q   Send-Q   Local Address:Port    Peer Address:Port  Rtt/var   Swnd  Retrans
ESTAB     0      257744      10.3.5.2:80         10.3.5.137:32963   530/15    13      0
```

```
ESTAB      0      861560      10.3.5.2:80         10.3.5.137:32849   545/24      4       0
ESTAB      0      234576      10.3.5.2:80         10.3.5.122:32979   547/22.2    6       0
ESTAB      0      254848      10.3.5.2:80         10.3.5.103:32909   531/14.8   10       0
ESTAB      0      231680      10.3.5.2:80         10.3.5.135:32925   532/11.5    9       0
ESTAB      0      224440      10.3.5.2:80         10.3.5.133:33057   550/32      7       0
ESTAB      0      267880      10.3.5.2:80         10.3.5.135:32985   530/18.2    7       0
ESTAB      0      291048      10.3.5.2:80         10.3.5.113:32909   539/12.2    6       0
ESTAB      0      249056      10.3.5.2:80         10.3.5.103:32903   520/23.2    8       0
ESTAB      0      218648      10.3.5.2:80         10.3.5.132:33069   522/14.5   16       0
ESTAB      0      702280      10.3.5.2:80         10.3.5.100:32829   539/24.5    5       0
ESTAB      0      412680      10.3.5.2:80         10.3.5.110:32992   546/22.8    7       0
ESTAB      0      254848      10.3.5.2:80         10.3.5.115:33136   552/37.2    5       0
```

Related Commands

Command	Description
gulp	Captures lossless gigabit packets and writes them to disk.
netmon	Displays the transmit and receive activity on an interface.
netstatr	Displays the rate of change of netstat statistics.
ss	Dumps socket statistics.

tcp

To configure TCP-related parameters, use the **tcp timestamp** command in global configuration mode. To disable the TCP timestamp, use the **no** form of this command.

tcp timestamp

no tcp timestamp

Syntax Description

timetstamp	Enables TCP timestamps.

Defaults

TCP timestamp is enabled by default.

Command Modes

Global configuration (config) mode.

Examples

The following example shows how to disable the TCP timestamp:

```
ServiceEngine# no tcp timestamp
ServiceEngine#
```

telnet (EXEC configuration)

To log in to a network device using the Telnet client, use the **telnet** command in EXEC configuration mode.

telnet {*hostname* | *ip_address*} [*port_num*]

Syntax Description

hostname	Hostname of the network device.
ip_address	IP address of the network device.
port_num	(Optional) Port number. The range is from 1 to 65535. Default port number is 23.

Defaults

The default port number is 23.

Command Modes

EXEC configuration mode.

Usage Guidelines

Some UNIX shell functions, such as escape and the **suspend** command, are not available in the Telnet client. In addition, multiple Telnet sessions are also not supported.

The Telnet client allows you to specify a destination port. By entering the **telnet** command, you can test websites by attempting to open a Telnet session to the website from the SE CLI.

Examples

The following example shows how to open a Telnet session to a network device using the hostname:

```
ServiceEngine# telnet cisco-ce
```

The following example shows how to open a Telnet session to a network device using the IP address:

```
ServiceEngine# telnet 172.16.155.224
```

The following example shows how to open a Telnet session to a network device on port 8443 using the hostname:

```
ServiceEngine# telnet cisco-ce 8443
```

The following example shows how to open a Telnet session to a network device on port 80 using the hostname:

```
ServiceEngine# telnet www.yahoo.com 80
```

telnet (global configuration)

To enable Telnet service, use the **telnet enable** command in global configuration mode. To disable Telnet, use the **no** form of this command.

telnet

no telnet

Syntax Description

enable	Enables Telnet service.

Defaults

Telnet is enabled by default.

Command Modes

Global configuration (config) mode.

Usage Guidelines

Use this Terminal Emulation protocol for a remote terminal connection. The **telnet enable** command allows users to log in to other devices using a Telnet session.

Examples

The following example shows how to enable Telnet on the SE:

```
ServiceEngine(config)# telnet enable
```

Related Commands

Command	Description
show telnet	Displays the Telnet services configuration.

terminal

To set the number of lines displayed in the console window, or to display the current console **debug** command output, use the **terminal** command in EXEC configuration mode.

terminal {**length** *length* | **monitor** [**disable**]}

Syntax Description

length	Sets the length of the display on the terminal.
length	Length of the display on the terminal (the range is 0 to 512). Setting the length to 0 means that there is no pausing.
monitor	Copies the debug output to the current terminal.
disable	(Optional) Disables monitoring at this specified terminal.

Defaults

The default length is 24 lines.

Command Modes

EXEC configuration mode.

Usage Guidelines

When 0 is entered as the *length* parameter, the output to the screen does not pause. For all nonzero values of *length*, the -More- prompt is displayed when the number of output lines matches the specified *length* number. The -More- prompt is considered a line of output. To view the next screen, press the **Spacebar**. To view one line at a time, press the **Enter** key.

The **terminal monitor** command allows a Telnet session to display the output of the **debug** commands that appear on the console. Monitoring continues until the Telnet session is terminated.

Examples

The following example shows how to set the number of lines to display to 20:

```
ServiceEngine# terminal length 20
```

The following example shows how to configure the terminal for no pausing:

```
ServiceEngine# terminal length 0
```

Related Commands

All **show** commands.

test-url

To test the accessibility of a URL using FTP, HTTP, or HTTPS, use the **test-url** command in EXEC configuration mode.

test-url {**ftp** *url* [**use-ftp-proxy** *proxy_url*] | **http** *url* [**custom-header** *header* [**head-only**] [**use-http-proxy** *proxy_url*] | **head-only** [**custom-header** *header*] [**use-http-proxy** *proxy_url*] | **use-http-proxy** *proxy_url* [**custom-header** *header*] [**head-only**]]}

Syntax Description

ftp	Specifies the File Transfer Protocol (FTP) URL to be tested.
url	FTP URL to be tested. Use one of the following formats to specify the FTP URL: • ftp://*domainname*/*path* • ftp://*user*:*password*@*domainname*/*path*
use-ftp-proxy	(Optional) Specifies the FTP proxy that is used to test the URL.
proxy_url	FTP proxy URL. Use one of the following formats to specify the proxy URL: • *proxy IP Address*:*proxy Port* • *proxy Username*:*proxy Password*@*proxy IP Address*:*proxy Port*
http	Specifies the HTTP URL to be tested.
url	HTTP URL to be tested. Use one of the following formats to specify the HTTP URL: • http://*domainname*/*path* • http://*user*:*password*@*domainname*/*path*
custom-header	(Optional) Specifies the custom header information to be sent to the server.
header	Custom header information to be sent to the server. Use the format *header*:*line* to specify the custom header.
head-only	(Optional) Specifies that only the HTTP header information must be retrieved.
use-http-proxy	(Optional) Specifies the HTTP proxy that is used to test the URL.
proxy_url	HTTP proxy URL. Use one of the following formats to specify the HTTP proxy URL: http://*proxyIp*:*proxyPort* http://*proxyUser*:*proxypasswd*@*proxyIp*:*proxyPort*
head-only	(Optional) Specifies that only the HTTPS header information must be retrieved.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The HTTP CLI client allows you to test connectivity and debug caching issues. The **test-url** command allows you to test whether a URL is accessible over the FTP, HTTP, and HTTPS protocols. When you test the connectivity using the **test-url** command, the SE sends a request using the protocol that you have specified to the server and fetches the requested contents. The actual content is dumped into the path /dev/null, and the server response with the header information is displayed to the user.

You can use the **test-url ftp** command to test the following for the specified URL:

- Connectivity to the URL
- Connectivity to the URL through the FTP proxy (using the **use-ftp-proxy** option)
- Authentication
- FTP proxy authentication

You can use the **test-url http** command to test the following for the specified URL:

- Test the connectivity to the URL
- Test the connectivity to the URL through the HTTP proxy (using the **use-http-proxy** option)
- Authentication
- HTTP proxy authentication
- Header information only for the specified page (using the **head-only** option) or additional header information (using the **custom-header** option)

Examples

The following example tests the accessibility to the URL http://192.168.171.22 using HTTP:

```
ServiceEngine# test-url http http://ce1.server.com
--02:27:20-- http://ce1.server.com/
           => `/dev/null'
Len - 22, Restval - 0, contlen - 0, Res - 134728056Resolving ce1.server.com. .

done.
Connecting to ce1.server.com [ 192.168.171.22 ] :80... connected.
HTTP request sent, awaiting response...
 1 HTTP/1.1 200 OK
 2 Date: Mon, 26 Jul 2004 08:41:34 GMT
 3 Server: Apache/1.2b8
 4 Last-Modified: Fri, 25 Apr 2003 12:23:04 GMT
 5 ETag: "1aee29-663-3ea928a8"
 6 Content-Length: 1635
 7 Content-Type: text/html
 8 Via: 1.1 Content Delivery System Software 5.2
 9 Connection: Keep-Alive
 (1635 to go)
 0% [                                    ] 0             --.--K/s    ETA --:--L
en - 0   ELen - 1635     Keepalive - 1
100% [ ====================================> ] 1,635          1.56M/s    ETA 00:00

02:27:20 (1.56 MB/s) - `/dev/null' saved [ 1635/1635 ]
```

The following example tests the accessibility to the URL http://192.168.171.22 through the HTTP proxy 10.107.192.148:

```
ServiceEngine# test-url http http://192.168.171.22 use-http-proxy 10.107.192.148:8090
--15:22:51-- http://10.77.155.246/
           => `/dev/null'
Len - 1393, Restval - 0, contlen - 0, Res - 134728344Connecting to 10.107.192.148:8090...
connected.
Proxy request sent, awaiting response...
```

```
 1 HTTP/1.1 401 Authorization Required
 2 Date: Mon, 27 Sep 2004 15:29:18 GMT
 3 Server: Apache/1.3.27 (Unix) tomcat/1.0
 4 WWW-Authenticate: Basic realm="IP/TV Restricted Zone"
 5 Content-Type: text/html; charset=iso-8859-1
 6 Via: 1.1 Content Delivery System Software 5.2.1
 7 Connection: Close
Len - 0, Restval - 0, contlen - -1, Res - -1Connecting to 10.107.192.148:8090...
connected.
Proxy request sent, awaiting response...
 1 HTTP/1.1 401 Authorization Required
 2 Date: Mon, 27 Sep 2004 15:29:19 GMT
 3 Server: Apache/1.3.27 (Unix) tomcat/1.0
 4 WWW-Authenticate: Basic realm="IP/TV Restricted Zone"
 5 Content-Type: text/html; charset=iso-8859-1
 6 Via: 1.1 Content Delivery System Software 5.2.1
 7 Connection: Keep-Alive
 (1635 to go)
 0% [                                    ] 0             --.--K/s    ETA --:--L
en - 0   ELen - 1635     Keepalive - 1
100% [ ====================================> ] 1,635          1.56M/s    ETA 00:00

02:27:20 (1.56 MB/s) - `/dev/null' saved [ 1635/1635 ]
```

The following example tests the accessibility to the URL ftp://ssivakum:ssivakum@10.77.157.148 using FTP:

```
ServeEngine# test-url ftp ftp://ssivakum:ssivakum@10.77.157.148/antinat-0.90.tar
Mar 30 14:33:44 nramaraj-ce admin-shell: %SE-PARSER-6-350232: CLI_LOG shell_parser_log:
test-url ftp ftp://ssivakum:ssivakum@10.77.157.148/antinat-0.90.tar
--14:33:44-- ftp://ssivakum:*password*@10.77.157.148/antinat-0.90.tar
           => `/dev/null'
Connecting to 10.77.157.148:21... connected.
Logging in as ssivakum...
220 (vsFTPd 1.1.3)
--> USER ssivakum

331 Please specify the password.
--> PASS Turtle Power!
230 Login successful. Have fun.
--> SYST

215 UNIX Type: L8
--> PWD

257 "/home/ssivakum"
--> TYPE I

200 Switching to Binary mode.
==> CWD not needed.
--> PORT 10,1,1,52,82,16

200 PORT command successful. Consider using PASV.
--> RETR antinat-0.90.tar

150 Opening BINARY mode data connection for antinat-0.90.tar (1771520 bytes).
Length: 1,771,520 (unauthoritative)

 0% [
 ] 0             --.--K/s    ETA --:--Len - 0   ELen - 1771520          Keepalive - 0
100%
[ ==========================================================================================> ]
1,771,520    241.22K/s    ETA 00:00
```

```
226 File send OK.
14:33:53 (241.22 KB/s) - `/dev/null' saved [ 1771520 ]

ServiceEngine#
```

Related Commands

Command	Description
acquirer (EXEC)	Starts or stops content acquisition on a specified acquirer delivery service.

top

To see a dynamic real-time view of a running VDS-OS, use the **top** command in EXEC configuration mode.

top {*line*}

Syntax Description

line	Specifies top options, enter **-h** to get Help. Press **q** to quit from the output.

Defaults

No default behavior values

Command Modes

EXEC configuration mode.

Examples

The following example shows sample output from the **top** command on an SE:

```
ServiceEngine# top
top - 01:08:45 up 8 days, 23:39, 3 users, load average: 1244.22, 1246.32, 1243.66
Tasks: 1789 total, 4 running, 1785 sleeping, 0 stopped, 0 zombie
Cpu(s): 0.0%us, 13.2%sy, 18.1%ni, 57.8%id, 1.1%wa, 0.7%hi, 9.2%si, 0.0%st
Mem: 32825728k total, 32671416k used, 154312k free, 137164k buffers
Swap:       0k total,        0k used,        0k free, 21289468k cached
```

traceroute

To trace the route to a remote host, use the **traceroute** command in EXEC configuration mode.

traceroute {*hostname* | *ip_address*}

Syntax Description

hostname	Name of the remote host.
ip_address	IP address of the remote host.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Traceroute is a widely available utility on most operating systems. Similar to ping, traceroute is a valuable tool for determining connectivity in a network. Ping allows the user to find out if there is a connection between the two end systems. Traceroute does this as well, but additionally lists the intermediate routers between the two systems. Users can see the routes that packets can take from one system to another. Use the **traceroute** command to find the route to a remote host when either the hostname or the IP address is known.

The **traceroute** command uses the Time-to-Live (TTL) field in the IP header to cause routers and servers to generate specific return messages. Traceroute starts by sending a UDP datagram to the destination host with the TTL field set to 1. If a router finds a TTL value of 1 or 0, it drops the datagram and sends back an Internet Control Message Protocol (ICMP) time-exceeded message to the sender. The traceroute facility determines the address of the first hop by examining the source address field of the ICMP time-exceeded message.

To identify the next hop, traceroute sends a UDP packet with a TTL value of 2. The first router decrements the TTL field by 1 and sends the datagram to the next router. The second router sees a TTL value of 1, discards the datagram, and returns the time-exceeded message to the source. This process continues until the TTL is incremented to a value large enough for the datagram to reach the destination host (or until the maximum TTL is reached).

To determine when a datagram has reached its destination, traceroute sets the UDP destination port in the datagram to a very large value that the destination host is unlikely to be using. When a host receives a datagram with an unrecognized port number, it sends an ICMP “port unreachable” error to the source. This message indicates to the traceroute facility that it has reached the destination.

Examples

The following example shows how to trace the route to a remote host from the SE:

```
ServiceEngine# traceroute 10.77.157.43
traceroute to 10.77.157.43 (10.77.157.43), 30 hops max, 38 byte packets
 1  10.1.1.50 (10.1.1.50) 2.024 ms 2.086 ms 2.219 ms
 2  sblab2-rtr.cisco.com (192.168.10.1) 3.718 ms 172.19.231.249 (172.19.231.249) 0.653 ms
0.606 ms
 3  sjc22-00lab-gw1.cisco.com (172.24.115.65) 0.666 ms 0.624 ms 0.597 ms
 4  sjc20-lab-gw2.cisco.com (172.24.115.109) 0.709 ms 0.695 ms 0.616 ms
 5  sjc20-sbb5-gw2.cisco.com (128.107.180.97) 0.910 ms 0.702 ms 0.674 ms
```

```
 6  sjc20-rbb-gw5.cisco.com (128.107.180.9) 0.762 ms 0.702 ms 0.664 ms
 7  sjc12-rbb-gw4.cisco.com (128.107.180.2) 0.731 ms 0.731 ms 0.686 ms
 8  sjc5-gb3-f1-0.cisco.com (10.112.2.158) 1.229 ms 1.186 ms 0.753 ms
 9  capnet-hkidc-sjc5-oc3.cisco.com (10.112.2.238) 146.784 ms 147.016 ms 147.051 ms
10  hkidc-capnet-gw1-g3-1.cisco.com (10.112.1.250) 147.163 ms 147.319 ms 148.050 ms
11  hkidc-gb3-g0-1.cisco.com (10.112.1.233) 148.137 ms 148.332 ms 148.361 ms
12  capnet-singapore-hkidc-oc3.cisco.com (10.112.2.233) 178.137 ms 178.273 ms 178.005 ms
13  singapore-capnet2-fa4-0.cisco.com (10.112.2.217) 179.236 ms 179.606 ms 178.714 ms
14  singapore-gb1-fa2-0.cisco.com (10.112.2.226) 179.499 ms 179.914 ms 179.873 ms
15  capnet-chennai-singapore-ds3.cisco.com (10.112.2.246) 211.858 ms 212.167 ms 212.854 ms
16  hclodc1-rbb-gw2-g3-8.cisco.com (10.112.1.213) 213.639 ms 212.580 ms 211.211 ms
17  10.77.130.18 (10.77.130.18) 212.248 ms 212.478 ms 212.545 ms
18  codc-tbd.cisco.com (10.77.130.34) 212.315 ms 213.088 ms 213.063 ms
19  10.77.130.38 (10.77.130.38) 212.955 ms 214.353 ms 218.169 ms
20  10.77.157.9 (10.77.157.9) 217.217 ms 213.424 ms 222.023 ms
21  10.77.157.43 (10.77.157.43) 212.750 ms 217.260 ms 214.610 ms
```

The following example shows how the **traceroute** command fails to trace the route to a remote host from the SE:

```
ServiceEngine# traceroute 10.0.0.1
traceroute to 10.0.0.1 (10.0.0.1), 30 hops max, 38 byte packets
 1  10.1.1.50 (10.1.1.50) 2.022 ms 1.970 ms 2.156 ms
 2  sblab2-rtr.cisco.com (192.168.10.1) 3.955 ms 172.19.231.249 (172.19.231.249) 0.654 ms
0.607 ms
 3  sjc22-00lab-gw1.cisco.com (172.24.115.65) 0.704 ms 0.625 ms 0.596 ms
 4  sjc20-lab-gw1.cisco.com (172.24.115.105) 0.736 ms 0.686 ms 0.615 ms
 5  sjc20-sbb5-gw1.cisco.com (128.107.180.85) 0.703 ms 0.696 ms 0.646 ms
 6  sjc20-rbb-gw5.cisco.com (128.107.180.22) 0.736 ms 0.782 ms 0.750 ms
 7  sjce-rbb-gw1.cisco.com (171.69.7.249) 1.291 ms 1.314 ms 1.218 ms
 8  sjce-corp-gw1.cisco.com (171.69.7.170) 1.477 ms 1.257 ms 1.221 ms
 9  * * *
10  * * *
.
.
.
29  * * *
30  * * *
```

Table 2-70 describes the fields in the **traceroute** command output.

Table 2-70 traceroute Command Output Fields

Field	Description
30 hops max, 38 byte packets	Maximum TTL value and the size of the ICMP datagrams being sent.
2.022 ms 1.970 ms 2.156 ms	Total time (in milliseconds) for each ICMP datagram to reach the router or host plus the time it took for the ICMP time-exceeded message to return to the host. An exclamation point following any of these values (for example, 20 ms) indicates that the port-unreachable message returned by the destination had a TTL of 0 or 1. Typically, this situation occurs when the destination uses the TTL value from the arriving datagram as the TTL in its ICMP reply. The reply does not arrive at the source until the destination receives a traceroute datagram with a TTL equal to the number of hops between the source and destination.
*	An asterisk (*) indicates that the timeout period (default of 5 seconds) expired before an ICMP time-exceeded message was received for the datagram.

Related Commands

Command	Description
ping	Sends echo packets for diagnosing basic network connectivity on networks.

traceroute6

To trace the route to a remote IPv6-enabled host, use the **traceroute6** command in EXEC configuration mode.

traceroute6 *ip_address*

Syntax Description

ip_address	Remote IPv6-enabled host or IP address.

Defaults

No default behavior values

Command Modes

EXEC configuration mode.

Examples

The following example shows how to trace the route to a remote IPv6-enabled host from the SE:

```
ServiceEngine# traceroute6 <IP address>
```

Related Commands

Command	Description
ipv6	Specifies the IPv6 address of the default gateway.

transaction-log force

To force the archive or export of the transaction log, use the **transaction-log force** command in EXEC configuration mode.

transaction-log force {**archive** | **export**}

Syntax Description

archive	Forces the archive of the *working.log* file.
export	Forces the archived files to be exported to the server.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

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

The **transaction-log force export** command causes the transaction log to be exported to a File Transfer Protocol (FTP) server designated by the **transaction-logs export ftp-server** command.

The **transaction-log force** command does not change the configured or default schedule for archive or export of transaction log files. If the archive interval is configured, in seconds, or the export interval is configured in minutes, the forced archive or export interval period is restarted after the forced operation.

If a scheduled archive or export job is in progress when a corresponding **transaction-log force** command is entered, the command has no effect. If a **transaction-log force** command is in progress when an archive or export job is scheduled to run, the forced operation is completed and the archive or export is rescheduled for the next configured interval.

Examples

The following example shows how to archive the transaction log file to the SE hard disk:

```
ServiceEngine# transaction-log force archive
```

The following example shows that the SE is configured to export its transaction logs to two FTP servers:

```
ServiceEngine(config)#  transaction-logs export ftp-server 10.1.1.1 mylogin mypasswd
/ftpdirectory
ServiceEngine(config)#  transaction-logs export ftp-server myhostname mylogin mypasswd
/ftpdirectory
```

The following example shows how to export the transaction log file from the SE hard disk to an FTP server designated by the **transaction-logs export ftp-server** command:

```
ServiceEngine# transaction-log force export
```

Related Commands

Command	Description
clear transaction logs	Clears the working transaction log settings.
show statistics transaction-logs	Displays the SE transaction log export statistics.
show transaction-logging	Displays the transaction log configuration settings and a list of archived transaction log files.
transaction-logs	Configures and enables the transaction logging parameters.

transaction-logs

To configure and enable transaction logs, use the **transaction-logs** command in global configuration mode. To disable transaction logs, use the **no** form of this command.

transaction-logs {**archive** {**interval** {*seconds* | **every-day** {**at** *hour:minute* | **every** *hours*} | **every-hour** {**at** *minute* | **every** *minutes*} | **every-week** [**on** *weekdays* **at** *hour:minute*]} | **max-file-number** *file_number* | **max-file-size** *file_size*} | **ds-snapshot-counter enable** | **enable** | **export** {**compress** | **enable** | **ftp-server** {*hostname* | *serv_ip_addrs*} *login passw directory* | **interval** {*minutes* | **every-day** {**at** *hour:minute* | **every** *hours*} | **every-hour** {**at** *minute* | **every** *minutes*} | **every-week** [**on** *weekdays* **at** *hour:minute*] | **sftp-server** {*hostname* | *serv_ip_addrs*} *login passw directory* | **format** {**apache** | **custom** *string* | **extended-squid**} | **log-windows-domain**}

no transaction-logs {**archive** {**interval** {*seconds* | **every-day** {**at** *hour:minute* | **every** *hours*} | **every-hour** {**at** *minute* | **every** *minutes*} | **every-week** [**on** *weekdays* **at** *hour:minute*]} | **max-file-number** *file_number* | **max-file-size** *file_size*} | **ds-snapshot-counter enable** | **enable** | **export** {**compress** | **enable** | **ftp-server** {*hostname* | *serv_ip_addrs*} *login passw directory* | **interval** {*minutes* | **every-day** {**at** *hour:minute* | **every** *hours*} | **every-hour** {**at** *minute* | **every** *minutes*} | **every-week** [**on** *weekdays* **at** *hour:minute*] | **sftp-server** {*hostname* | *serv_ip_addrs*} *login passw directory* | **format** {**apache** | **custom** *string* | **extended-squid**} | **log-windows-domain**}

Syntax Description

archive	Configures archive parameters.
interval	Determines how frequently the archive file is to be saved.
seconds	Frequency of archiving, in seconds. The range is from120 to 604800.
every-day	Archives using intervals of 1 day or less.
at	Specifies the local time at which to archive each day.
hour:minute	Time of day at which to archive in local time (hh:mm).
every	Specifies the interval in hours. Interval aligns with midnight.
hours	Number of hours for daily file archive. 1—Hourly 12—Every 12 hours 2—Every 2 hours 24—Every 24 hours 3—Every 3 hours 4—Every 4 hours 6—Every 6 hours 8—Every 8 hours
every-hour	Specifies the archives using intervals of 1 hour or less.
at	Sets the time to archive at each hour.
minute	Minute alignment for the hourly archive. The range is from 0 to 59.
every	Specifies the interval in minutes for hourly archive that aligns with the top of the hour.

minutes	Number of minutes for hourly archive. 10—Every 10 minutes 15—Every 15 minutes 2—Every 2 minutes 20—Every 20 minutes 30—Every 30 minutes 5—Every 5 minutes
every-week	Archives using intervals of 1 or more times a week.
on	(Optional) Sets the day of the week on which to archive.
weekdays	Weekdays on which to archive. One or more weekdays can be specified. Fri—Every Friday Mon—Every Monday Sat—Every Saturday Sun—Every Sunday Thu—Every Thursday Tue—Every Tuesday Wed—Every Wednesday
at	(Optional) Sets the local time at which to archive each day.
hour:minute	Time of day at which to archive in local time (hh:mm).
max-file-number	Sets the maximum number of the archived log file.
file_number	Maximum number of the archived log file. The range is from 1 to 10000.
max-file-size	Sets the maximum archive file size.
filesize	Maximum archive file size in kilobytes. The range is from 1000 to 2000000.
ds-snapshot-counter enable	Enables the per delivery service snapshot counter.
enable	Enables the transaction log.
export	Configures file export parameters.
compress	Compresses the archived files in the gzip format before exporting.
enable	Enables the exporting of log files at the specified interval.
ftp-server	Sets the File Transfer Protocol (FTP) server to receive exported archived files.
hostname	Hostname of the target FTP server.
serv_ip_addrs	IP address of the target FTP server.
login	User login to target FTP server.
passw	User password to target FTP server.
directory	Target directory path for exported files on FTP server.
interval	Determines how frequently the file is to be exported.
minutes	Number of minutes in the interval at which to export a file. The range is from 1 to 10080.
every-day	Specifies the exports using intervals of 1 day or less.
at	Specifies the local time at which to export each day.
hour:minute	Time of day at which to export in local time (hh:mm).
every	Specifies the interval in hours for the daily export.

hours	Number of hours for the daily export. 1—Hourly 12—Every 12 hours 2— Every 2 hours 24—Every 24 hours 3— Every 3 hours 4—Every 4 hours 6—Every 6 hours 8—Every 8 hours
every-hour	Specifies the exports using intervals of 1 hour or less.
at	Specifies the time at which to export each hour.
minute	Minute alignment for the hourly export. The range is from 0 to 59.
every	Specifies the interval in minutes that align with the top of the hour.
minutes	Number of minutes for the hourly export. 10—Every 10 minutes 15—Every 15 minutes 2—Every 2 minutes 20—Every 20 minutes 30—Every 30 minutes 5—Every 5 minutes
every-week	Specifies the exports using intervals of 1 of more times a week.
on	(Optional) Specifies the days of the week for the export.
weekdays	Weekdays on which to export. One or more weekdays can be specified. Fri—Every Friday Mon—Every Monday Sat—Every Saturday Sun—Every Sunday Thu—Every Thursday Tue—Every Tuesday Wed—Every Wednesday
at	(Optional) Specifies the time of day at which to perform the weekly export.
hour:minute	Time of day at which to export in the local time (hh:mm).
sftp-server	Sets the Secure File Transfer Protocol (SFTP) server to receive exported archived files.
hostname	Hostname of the target SFTP server.
serv_ip_addrs	IP address of the target SFTP server.
login	User login to the target SFTP server (less than 40 characters).
passw	User password to the target SFTP server (less than 40 characters).
directory	Target directory path for exported files on the SFTP server.
format	Sets the format to use for the HTTP transaction log entries in the working.log file.
apache	Configures the HTTP transaction logs output to the Apache common log format (CLF).
custom	Configures the HTTP transaction logs output to the custom log format.
string	Quoted log format string containing the custom log format.

extended-squid	Configures the HTTP transaction logs output to the Extended Squid log format.
log-windows-domain	Logs the Windows domain with an authenticated username if available in HTTP transaction log entries.
enable	Enables the remote transaction logging.
entry-type	Specifies the type of transaction log entry.
all	Sets the SE to send all transaction log messages to the remote syslog server.
request-auth-failures	Sets the SE to log to the remote syslog server only those transactions that the SE failed to authenticate with the Authentication Server. **Note** Only those authentication failures that are associated with an end user who is attempting to contact the Authentication Server are logged. The transactions in pending state (that have contacted the Authentication Server, but waiting for a response from the Authentication Server) are not logged.
facility	Configures a unique facility to create a separate log on the remote syslog host for real-time transaction log entries.
parameter	Specifies one of the following facilities: auth—Authorization system daemon—System daemons kern—Kernel local0—Local use local1—Local use local2—Local use local3—Local use local4—Local use local5—Local use local6—Local use local7—Local use mail—Mail system news—USENET news syslog—Syslog itself user—User process uucp—UUCP system
host	Configures the remote syslog server.
hostname	Hostname of the remote syslog server.
ip-address	IP address of the remote syslog server.
port	Configures the port to use when sending transaction log messages to the syslog server.
port-num	Port number to use when sending transaction log messages to the syslog server. The default is 514.
rate-limit	Configures the rate at which the transaction logger is allowed to send messages to the remote syslog server.
rate	Rate (number of messages per second) at which the transaction logger is allowed to send messages to the remote syslog server.

Defaults

archive: disabled

enable: disabled

export compress: disabled

export: disabled

file-marker: disabled

archive interval: every day, every one hour

archive max-file-size: 2,000,000 KB

export interval: every day, every one hour

format: apache

logging port *port_num*: 514

Command Modes

Global configuration (config) mode.

Usage Guidelines

SEs can record all errors and access activities. Each content service module on the SE provides logs of the requests that were serviced. These logs are referred to as transaction logs.

Typical fields in the transaction log are the date and time when a request was made, the URL that was requested, whether it was a cache hit or a cache miss, the type of request, the number of bytes transferred, and the source IP address. Transaction logs are used for problem identification and solving, load monitoring, billing, statistical analysis, security problems, and cost analysis and provisioning.

The translog module on the SE handles transaction logging and supports the Apache CLF, Extended Squid format, and the World Wide Web Consortium (W3C) customizable logging format.

Note For Real-Time Streaming Protocol (RTSP), when you choose the **Repeat** option from the Play menu in the Windows Media player to play media files continuously in a loop, an extra entry is logged in the transaction logs for each playback of the file.

Enable transaction log recording with the **transaction-logs enable** command. The transactions that are logged include HTTP and File Transfer Protocol (FTP). In addition, Extensible Markup Language (XML) logging for MMS-over-HTTP and MMS-over-RTSP (RTSP over Windows Media Services 9) is also supported.

When enabled, daemons create a *working.log* file in /local1/logs/ on the system file system (sysfs) volume for HTTP and FTP transactions and a separate *working.log* file in /local1/logs/export for Windows Media transactions.

The *working.log* file is a link to the actual log file with the timestamp embedded in its filename. When you configure the **transaction-logs archive interval** command, the first transaction that arrives after the interval elapses is logged to the *working.log* file as usual, and then actual log file is archived and a new log file is created. Only transactions subsequent to the archiving event are recorded in the new log file. The *working.log* file is then updated to point to the newly created log file. The transaction log archive file naming conventions are shown in Table 2-71. The SE default archive interval is once an hour every day.

Note The time stamp in the transaction log filename is in Coordinated Universal Time (UTC) and is irrespective of the time zone configured on the SE. The time stamp in the transaction log filename is the time when the file was created. The logs entries in the transaction logs are in the time zone configured on the SE.

Use the **transaction-logs ds-snapshot-counter enable** command to enable or disable snapshot counter transaction logs. This command is available for both SE and SR. On SE, the snapshot counter transaction log records per delivery service Storage Usage. On the SR, the snapshot counter transaction log records per delivery service Session and Bandwidth Usage.

Use the **transaction-logs archive max-file-size** command to specify the maximum size of an archive file. The *working.log* file is archived when it attains the maximum file size if this size is reached before the configured archive interval time.

Use the **transaction-logs file-marker** option to mark the beginning and end of the HTTP, HTTPS, and FTP proxy logs. By examining the file markers of an exported archive file, you can determine whether the FTP process transferred the entire file. The file markers are in the form of dummy transaction entries that are written in the configured log format.

The following example shows the start and end dummy transactions in the default native Squid log format.

- 970599034.130 0 0.0.0.0 TCP_MISS/000 0 NONE TRANSLOG_FILE_START - NONE/- -
- 970599440.130 0 0.0.0.0 TCP_MISS/000 0 NONE TRANSLOG_FILE_END - NONE/- -

Use the **format** option to format the HTTP, HTTPS, and FTP proxy log files for custom format, native Squid or Extended Squid formats, or Apache CLF.

The **transaction-logs format custom** command allows you to use a *log format string* to log additional fields that are not included in the predefined native Squid or Extended Squid formats or the Apache CLF. The *log format string* is a string that contains the tokens listed in Table 2-71 and mimics the Apache log format string. The log format string can contain literal characters that are copied into the log file. Two backslashes (\\) can be used to represent a literal backslash, and a backslash followed by a single quotation mark (\') can be used to represent a literal single quotation mark. A literal double quotation mark cannot be represented as part of the log format string. The control characters \t and \n can be used to represent a tab and a new line character, respectively.

Table 2-71 lists the acceptable format tokens for the log format string. The ellipsis (...) portion of the format tokens shown in this table represent an optional condition. This portion of the format token can be left blank, as in %a. If an optional condition is included in the format token and the condition is met, then what is shown in the Value column of Table 2-71 is included in the transaction log output. If an optional condition is included in the format token but the condition is not met, the resulting transaction log output is replaced with a hyphen (-). The form of the condition is a list of HTTP status codes, which may or may not be preceded by an exclamation point (!). The exclamation point is used to negate all the status codes that follow it, which means that the value associated with the format token is logged if none of the status codes listed after the exclamation point (!) match the HTTP status code of the request. If any of the status codes listed after the exclamation point (!) match the HTTP status code of the request, then a hyphen (-) is logged.

For example, %400,501 { User-Agent } i logs the User-Agent header value on 400 errors and 501 errors (Bad Request, Not Implemented) only, and %!200,304,302 { Referer } i logs the Referer header value on all requests that did not return a normal status.

The custom format currently supports the following request headers:

- User-Agent
- Referer
- Host
- Cookie

The output of each of the following Request, Referer, and User-Agent format tokens specified in the custom *log format string* is always enclosed in double quotation marks in the transaction log entry:

%r

% { Referer } i

% { User-Agent } i

The % { Cookie } i format token is generated without the surrounding double quotation marks, because the Cookie value can contain double quotes. The Cookie value can contain multiple attribute-value pairs that are separated by spaces. We recommend that when you use the Cookie format token in a custom format string, you should position it as the last field in the format string so that it can be easily parsed by the transaction log reporting tools. By using the format token string \'% { Cookie } i\' the Cookie header can be surrounded by single quotes (').

Note Each transaction log includes a header line that provides the VDS-OS software version and a summary line as the last line in the transaction log, which includes a summary of all the requests that appear in the transaction log.

The following command can generate the well-known Apache Combined Log Format:

transaction-log format custom " [**% { %d } t/% { %b } t/% { %Y } t:% { %H } t:% { %M } t:% { %S } t % { %z } t] %r %s %b % { Referer } i % { User-Agent } i"**

The following transaction log entry example in the Apache Combined Format is configured using the preceding custom format string:

```
 [ 11/Jan/2003:02:12:44 -0800 ] "GET http://www.cisco.com/swa/i/site_tour_link.gif
HTTP/1.1" 200 3436 "http://www.cisco.com/" "Mozilla/4.0 (compatible; MSIE 5.5; Windows NT
5.0)"
```

Table 2-71 Custom Format Log Format String Values

Format Token	Value
%a	IP address of the requesting client.
%A	IP address of the SE.
%b	Bytes sent, excluding HTTP headers.
%c	Log Entry Generation Time.
%C	Records AuthLOOKupTime|CALLOOKuptime|CacheRouterTime|OSDownload Time in microseconds.
%D	Time consumed to serve the request in microseconds.
%g	Storage URL when URL Resolve rule action is configured in Service Rule file.
%G	Source URL when URL Resolve rule action is configured in Service Rule file.
%h	Remote host (IP address of the requesting client is logged).
%H	Request protocol.

Table 2-71 Custom Format Log Format String Values (continued)

Format Token	Value
%I	Bytes received from the client.
%J	Gives the average RTT (Round trip time) for that transaction.
%K	Gives the congestion window flickers for the transaction.
%L	Prints the asset size, irrespective of the bytes transferred.
%m	Request method.
%M	MIME type of the requested asset.
%N	The network interface and bytes transferred in that interface.
%O	Bytes sent to client, including the headers.
%p	The client who set up the transport session for the request.
%q	Query string (which is preceded by a question mark (?) if a query string exists; otherwise, it is an empty string).
%r	First line of the request. The space in the first line of the request is replaced with a vertical bar (|) delimiter (for example, Getl/index.html|HTTP/1.1)
%R	Request description (Squid description codes).
%s	Status. The translog code always returns the HTTP response code for the request.
%t	Time in common log time format (or standard English format).
%T	Time consumed to serve the request in seconds (a floating point number with 3 decimal places).
%u	URL path requested, including query strings.
%U	URL path requested, not including query strings.
%V	Value of the host request header field reported if the host appeared in the request. If the host did not appear in the host request header, the IP address of the server specified in the URL is reported.
%X	Connection status when the response is completed. The %X field has the following possible values: X-Connection aborted before the response completed. + -Connection may be kept alive after the response is sent. - -Connection is closed after the response is sent.
%Z	Print the request received time stamp in milliseconds; otherwise, the request received time stamp is in seconds.
%{Header-Field}i	Any request header. Replace the Header-Field with the actual header field you want to log; for example, %{Cache-Control}i. **Note** All client request headers are only logged on the edge SE.

Sanitizing Transaction Logs

Use the **sanitized** option to disguise the IP address of clients in the transaction log file. The default is that transaction logs are not sanitized. A sanitized transaction log disguises the network identity of a client by changing the IP address in the transaction logs to 0.0.0.0.

The **no** form of this command disables the sanitize feature. The **transaction-logs sanitize** command does not affect the client IP (%a) value associated with a custom log format string that is configured with the CLI (configured with the **transaction-logs format custom** *string* command in global configuration mode in which the string is the quoted log format string that contains the custom log format). To hide the identity of the client IP in the custom log format, either hard code 0.0.0.0 in the custom log format string or exclude the %a token, which represents the client IP, from the format string.

Exporting Transaction Log Files

To facilitate the postprocessing of cache log files, you could export transaction logs to an external host.

This feature allows log files to be exported automatically by File Transfer Protocol (FTP) to an external host at configurable intervals. The username and password used for FTP are configurable. The directory to which the log files are uploaded is also configurable.

The log files automatically have the following naming convention:

- Module name
- Host IP address
- Date
- Time
- File generation number

For example, the filename for a Web Engine access log would be the following:

```
we_accesslog_apache_192.0.2.22_20091207_065624_00001
```

where we_accesslog_apache is the module name, 192.0.2.22 is the IP address of the device, 20091207 is the date of the log file (December 7, 2009), and 065624_00001 is the file generation number. The file generation number ranges from 00001 to 99999.

Exporting and Archiving Intervals

The transaction log archive and export functions are configured with the following commands:

- The **transaction-logs archive interval** command in global configuration mode allows the administrator to specify when the *working.log* file is archived.
- The **transaction-logs export interval** command in global configuration mode allows the administrator to specify when the archived transaction logs are exported.

The following limitations apply:

- When the interval is scheduled in units of hours, the value must divide evenly into 24. For example, the interval can be every 4 hours, but not every 5 hours.
- When the interval is scheduled in units of minutes, the value must divide evenly into 60.
- Only the more common choices of minutes are supported. For example, the interval can be 5 minutes or 10 minutes, but not 6 minutes.
- Selection of interval alignment is limited. If an interval is configured for every 4 hours, it aligns with midnight. It cannot align with 12:30 or with 7 a.m.
- Feature does not support different intervals within a 24-hour period. For example, it does not support an interval that is hourly during regular business hours and then every 4 hours during the night.

Transaction Log Archive Filenaming Convention

The archive transaction log file is named as follows for HTTP caching:

```
celog_10.1.118.5_20001228_235959.txt
```

```
mms_export_10.1.118.5_20001228_235959
```

If the **export compress** feature is enabled when the file is exported, then the file extension is *.gz* after the file is compressed for the export operation, as shown in the following example:

```
celog_10.1.118.5_20001228_235959.txt.gz

mms_export_10.1.118.5_20001228_235959.gz
```

Table 2-72 describes the name elements.

Table 2-72 Archive Log Name Element Descriptions

Sample of Element	Description
acqdist_	Acquisition and distribution archive log file.
cseaccess	Cisco Streaming Engine archive file.
tftp_server_	Trivial File Transfer Protocol (TFTP) server archive file.
webengine_apache	Web Engine Apache transaction logging format log file.
webengine_clf	Web Engine custom transaction logging format log file.
webengine_extsquid	Web Engine extended-squid transaction logging format log file.
cache_content	Content Access Layer transaction log file.
authsvr	VDS-OS Authorization Server transaction log file.
mms_export_	Standard Windows Media Services 4.1 caching proxy server archive file.
mms_export_e_wms_41_	Extended Windows Media Services 4.1 caching proxy server archive file.
mms_export_wms_90_	Standard Windows Media Services 9.0 caching proxy server archive file.
mms_export_e_wms_90_	Extended Windows Media Services 9.0 caching proxy server archive file.
10.1.118.5_	IP address of the SE creating the archive file.
20001228_	Date on which the archive file was created (yyyy/mm/dd).
235959	Time when the archive file was created (hh/mm/ss).

Table 2-73 lists the directory names and the corresponding examples of the archive filenames.

Table 2-73 Archive Filename Examples and Directories

Directory	Archive Filename
logs/acqdist	acqdist_10.1.94.4_20050315_001545
logs/cisco-streaming-engine	cseaccess10.1.94.4__050315000.log
logs/tftp_server	tftp_server_10.1.94.4_20050315_001545
logs/webengine_apache	we_accesslog_apache_114.0.92.27_20110322_213143_00001
logs/webengine_clf	we_accesslog_clf_114.0.92.27_20110322_213143_00004
logs/webengine_extsquid	we_accesslog_extsqu_114.0.92.27_20110322_213143_00072
logs/cache_content	cache_content_10.1.94.4_20110323_210446_00001
logs/authsvr	authsvr_10.1.94.4_20110323_210446_00001
logs/export	mms_export_18.0.101.116_20110318_121111_00120

Table 2-73 Archive Filename Examples and Directories (continued)

Directory	Archive Filename
logs/export/extended-wms-41	mms_export_e_wms_41_18.0.101.116_20110318_012847_00001
logs/wms-90	mms_export_wms_90_18.0.101.116_20110318_012847_00001
logs/export/extended-wms-90	mms_export_e_wms_90_18.0.101.116_20110318_012847_00001

Compressing Archive Files

The **transaction-logs export compress** option compresses an archive into a gzip file format before exporting it. Compressing the archive file uses less disk space on both the SE and the File Transfer Protocol (FTP) export server. The compressed file uses less bandwidth when transferred. The archive filename of the compressed file has the extension *.gz*.

Exporting Transaction Logs to External FTP Servers

The **transaction-logs export ftp-server** option can support up to four FTP servers. To export transaction logs, first enable the feature and configure the FTP server parameters. The following information is required for each target FTP server:

- FTP server IP address or the hostname

  The SE translates the hostname with a Domain Name System (DNS) lookup and then stores the IP address in the configuration.

- FTP user login and user password
- Path of the directory where transferred files are written

  Use a fully qualified path or a relative path for the user login. The user must have write permission to the directory.

Use the **no** form of the **transaction-logs export enable** command to disable the entire transaction logs feature while retaining the rest of the configuration.

Exporting Transaction Logs to External SFTP Servers

Use the **transaction-logs export sftp-server** option to export transaction logs. First enable the feature and configure the Secure File Transfer Protocol (SFTP) server parameters. The following information is required for each target SFTP server:

- SFTP server IP address or the hostname

  The SE translates the hostname with a DNS lookup and then stores the IP address in the configuration.

- SFTP user login and user password
- Path of the directory where transferred files are written

  Use a fully qualified path or a relative path for the user login. The user must have write permission to the directory.

Use the **no** form of the **transaction-logs export enable** command to disable the entire transaction logs feature while retaining the rest of the configuration.

Receiving a Permanent Error from the External FTP Server

A permanent error (Permanent Negative Completion Reply, RFC 959) occurs when the FTP command to the server cannot be accepted, and the action does not take place. Permanent errors can be caused by invalid user logins, invalid user passwords, and attempts to access directories with insufficient permissions.

When an FTP server returns a permanent error to the SE, the export is retried at 10-minute intervals or sooner if the configured export interval is sooner. If the error is a result of a misconfiguration of the **transaction-logs export ftp server** command, then re-enter the SE parameters to clear the error condition. The **show statistics transaction-logs** command displays the status of logging attempts to export servers.

The **show statistics transaction-logs** command shows that the SE failed to export archive files.

The **transaction-logs format** command has three options: **extended-squid**, **apache**, and **custom**.

Use the **no** form of the **transaction-logs export enable** command to disable the entire transaction logs feature while retaining the rest of the configuration.

Configuring Intervals Between 1 Hour and 1 Day

The archive or export interval can be set for once a day with a specific time stamp. It can also be set for hour frequencies that align with midnight. For example, every 4 hours means archiving occurs at 0000, 0400, 0800, 1200, and 1600. It is not possible to archive at half-hour intervals such as 0030, 0430, or 0830. The following intervals are acceptable: 1, 2, 3, 4, 6, 8, 12, and 24.

Configuring Intervals of 1 Hour or Less

The interval can be set for once an hour with a minute alignment. It can also be set for frequencies of less than an hour; these frequencies align with the top of the hour. Every 5 minutes means that archiving occurs at 1700, 1705, and 1710.

Configuring Export Interval on Specific Days

The export interval can be set for specific days of the week at a specific time. One or more days can be specified. The default time is midnight.

Archived logs are automatically deleted when free disk space is low. It is important to select an export interval that exports files frequently enough so that files are not automatically removed before export.

Monitoring HTTP Request Authentication Failures in Real Time

HTTP transaction log messages are sent to a remote syslog server so that you can monitor the remote syslog server for HTTP request authentication failures in real time. This real-time transaction log allows you to monitor transaction logs in real time for particular errors such as HTTP request authentication errors. The existing transaction logging to the local file system remains unchanged.

Note Because system logging (syslog) occurs through UDP, the message transport to the remote syslog host is not reliable.

Summary Line

The transaction logs include a summary line as the last line in the transaction log, which includes a summary of all the requests that appear in the transaction log.

Examples

The following example shows how to configure an FTP server:

```
ServiceEngine(config)# transaction-logs export ftp-server 10.1.1.1 mylogin mypasswd
/ftpdirectory

ServiceEngine(config)# transaction-logs export ftp-server myhostname mylogin mypasswd
/ftpdirectory
```

The following example shows how to delete an FTP server:

```
ServiceEngine(config)# no transaction-logs export ftp-server 10.1.1.1
ServiceEngine(config)# no transaction-logs export ftp-server myhostname
```

Use the **no** form of the command to disable the entire transaction log export feature while retaining the rest of the configuration:

```
ServiceEngine(config)# no transaction-logs export enable
```

The following example shows how to change a username, password, or directory:

```
ServiceEngine(config)# transaction-logs export ftp-server 10.1.1.1 mynewname mynewpass
/newftpdirectory
```

Note For security reasons, passwords are never displayed.

The following example shows how to restart the export of archive transaction logs:

```
ServiceEngine(config)# transaction-logs export ftp-server 172.16.10.5 goodlogin pass
/ftpdirectory
```

The following example shows how to delete an SFTP server from the current configuration:

```
ServiceEngine(config)# no transaction-logs export sftp-server sftphostname
```

The following examples show how to configure the archiving intervals:

```
ServiceEngine(config)# transaction-logs archive interval every-day
  at        Specify the time at which to archive each day
  every     Specify the interval in hours. It will align with midnight

ServiceEngine(config)# transaction-logs archive interval every-day at
<0-23>:  Time of day at which to archive (hh:mm)

ServiceEngine(config)# transaction-logs archive interval every-day every
<1-24>  Interval in hours: { 1, 2, 3, 4, 6, 8, 12 or 24 }
```

The following example shows that the SE has failed to export archive files:

```
ServiceEngine# show statistics transaction-logs
Transaction Log Export Statistics:

Server:172.16.10.5
      Initial Attempts:1
      Initial Successes:0
      Initial Open Failures:0
      Initial Put Failures:0
      Retry Attempts:0
      Retry Successes:0
      Retry Open Failures:0
      Retry Put Failures:0
      Authentication Failures:1
      Invalid Server Directory Failures:0
```

The following example shows how to correct a misconfiguration:

```
ServiceEngine(config)# transaction-logs export ftp-server 10.1.1.1 goodlogin pass
/ftpdirectory
```

The working.log file and archived log files are listed for HTTP.

The following example shows how to export transaction logs to an SFTP server:

```
ServiceEngine(config)# transaction-logs export sftp-server 10.1.1.100 mylogin mypasswd
/mydir
```

The following example shows how to archive every 4 hours and align with the midnight local time (0000, 0400, 0800, 1200, 1600, and 2000):

```
ServiceEngine(config)# transaction-logs archive interval every-day every 4
```

The following example shows how to export once a day at midnight local time:

```
ServiceEngine(config)# transaction-logs export interval every-day every 24
```

The following example shows how to configure export intervals:

```
ServiceEngine(config)# transaction-logs archive interval every-hour ?
  at        Specify the time at which to archive each day
  every     Specify interval in minutes. It will align with top of the hour

ServiceEngine(config)# transaction-logs archive interval every-hour at ?
  <0-59>  Specify the minute alignment for the hourly archive
ServiceEngine(config)# transaction-logs archive interval every-hour every ?
  <2-30>  Interval in minutes: { 2, 5, 10, 15, 20, 30 }
```

Related Commands

Command	Description
clear transaction-log	Clears the working transaction log settings.
show statistics transaction-logs	Displays the SE transaction log export statistics.
show transaction-logging	Displays the transaction log configuration settings and a list of archived transaction log files.
transaction-log force	Forces the archive or export of the transaction log.

type

To display the contents of a file, use the **type** command in EXEC configuration mode.

type *filename*

Syntax Description

filename	Name of file.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use this command to display the contents of a file within any SE file directory. This command may be used to monitor features such as transaction logging or system logging (syslog).

Examples

The following example shows how to display the syslog file on the SE:

```
ServiceEngine# type /local1/syslog.txt

Jan 10 22:02:46 (none) populate_ds: %SE-CLI-5-170050: VDS-OS Software starts booting
Jan 10 22:02:47 (none) create_etc_hosts.sh: %SE-CLI-5-170051: HOSTPLUSDOMAIN: NO-HOSTNAME
Jan 10 22:02:47 NO-HOSTNAME : %SE-CLI-5-170053: Recreated etc_hosts (1, 0)
Jan 10 22:02:48 NO-HOSTNAME Nodemgr: %SE-NODEMGR-5-330082: [ CLI_VER_NTP ] requests stop
service ntpd
Jan 10 22:02:49 NO-HOSTNAME Nodemgr: %SE-NODEMGR-5-330082: [ ver_tvout ] requests stop
service tvoutsvr
Jan 10 22:02:50 NO-HOSTNAME Nodemgr: %SE-NODEMGR-5-330084: [ ver_rtspg ] requests restart
service rtspg
Jan 10 22:02:50 NO-HOSTNAME Nodemgr: %SE-NODEMGR-5-330082: [ ver_iptv ] requests stop
service sbss
Jan 10 22:02:51 NO-HOSTNAME Nodemgr: %SE-NODEMGR-5-330080: [ ver_telnetd ] requests start
service telnetd
Jan 10 22:02:55 NO-HOSTNAME Nodemgr: %SE-NODEMGR-5-330082: [ Unknown ] requests stop
service mcast_sender
Jan 10 22:02:55 NO-HOSTNAME Nodemgr: %SE-NODEMGR-5-330082: [ Unknown ] requests stop
service mcast_receiver
Jan 10 22:02:56 NO-HOSTNAME Nodemgr: %SE-NODEMGR-5-330024: Service 'populate_ds' exited
normally with code 0
Jan 10 22:02:56 NO-HOSTNAME Nodemgr: %SE-NODEMGR-5-330040: Start service 'parser_server'
using: '/ruby/bin/parser_server' with pid: 1753
Jan 10 22:02:56 NO-HOSTNAME Nodemgr: %SE-NODEMGR-5-330040: Start service
'syslog_bootup_msgs' using: '/ruby/bin/syslog_bootup_msgs' with pid:
1754
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4>Linux version 2.4.16
(cnbuild@builder2.cisco.com) (gcc version 3.0.4) # 1
SMP Fri Jan 7 19:26:58 PST 2005
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <6>setup.c: handling
flash window at [ 15MB. .16MB)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <6>BIOS-provided
physical RAM map:
```

```
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4> BIOS-e820:
0000000000000000 - 000000000009ec00 (usable)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4> BIOS-e820:
000000000009ec00 - 00000000000a0000 (reserved)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4> BIOS-e820:
00000000000e0800 - 0000000000100000 (reserved)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4> BIOS-e820:
0000000000100000 - 00000000f00000 (usable)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4> BIOS-e820:
00000000f00000 - 0000000001000000 (reserved)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4> BIOS-e820:
0000000001000000 - 0000000010000000 (usable)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4> BIOS-e820:
00000000fff00000 - 0000000100000000 (reserved)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <6>setup.c: reserved
bootmem for INITRD_START = 0x6000000, INITRD_SIZE = 117
09348
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4>On node 0 totalpages:
65536
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4>zone(0): 4096 pages.
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4>zone(1): 61440 pages.
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4>zone(2): 0 pages.
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4>Local APIC disabled
by BIOS -- reenabling.
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4>Found and enabled
local APIC!
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4>Kernel command line:
root=/dev/ram ramdisk_size=100000 ramdisk_start=0x60
00000 console=ttyS0,9600n8
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <6>Initializing CPU# 0
<output truncated>
```

Related Commands

Command	Description
cpfile	Copies a file.
dir	Displays the files in a directory in a long-list format.
lls	Displays a long list of directory names.
ls	Lists the files and subdirectories in a directory.
mkfile	Makes a file (for testing).

type-tail

To view a specified number of lines of the end of a log file or to view the end of the file continuously as new lines are added to the file, use the **type-tail** command in EXEC configuration mode.

type-tail *filename* [*line* | **follow**]

Syntax Description

filename	File to be examined.
line	(Optional) The number of lines from the end of the file to be displayed (the range is 1 to 65535).
follow	(Optional) Displays the end of the file continuously as new lines are added to the file.

Defaults

The default is ten lines shown.

Command Modes

EXEC configuration mode.

Usage Guidelines

This command allows you to monitor a log file by letting you view the end of the file. You can specify the number of lines at the end of the file that you want to view, or you can follow the last line of the file as it continues to log new information. To stop the last line from continuously scrolling, press **Ctrl-C**.

Examples

The following example shows the list of log files in the /local1 directory:

```
stream-ServiceEngine# ls /local1
WS441
Websense
WebsenseEnterprise
Websense_config_backup
WsInstallLog
badfile.txt
codecoverage
core.stunnel.5.3.0.b100.cnbuild.5381
core_dir
crash
crka.log
cse_live
cse_vod
dbdowngrade.log
dbupgrade.log
downgrade
errorlog
http_authmod.unstrip
index.html
logs
lost+found
netscape-401-proxy
netscape-401-proxy1
netscape-dump
newwebsense
oldWsInstallLog
preload_dir
```

```
proxy-basic1
proxy1
proxy2
proxy3
proxy4
proxy5
proxy6
proxy7
proxy8
proxyreply
proxyreply-407
real_vod
ruby.bin.cli_fix
ruby.bin.no_ws_fix
ruby.bin.ws_edir_fix
sa
service_logs
smartfilter
smfnaveen
superwebsense
syslog.txt
syslog.txt.1
syslog.txt.2
temp
two.txt
url.txt
urllist.txt
var
vpd.properties
websense.pre-200
webtarball44
webtarball520
ws_upgrade.log
```

The following example shows how to display the last ten lines of the syslog.txt file. In this example, the number of lines to display is not specified; however, ten lines is the default.

```
stream-ServiceEngine# type-tail /local1/syslog.txt
Oct 8 21:49:15 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct 8 21:49:15 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct 8 21:49:15 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct 8 21:49:17 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct 8 21:49:17 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct 8 21:49:17 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct 8 21:49:19 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct 8 21:49:19 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct 8 21:49:19 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct 8 21:49:21 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
```

The following example shows how to display the last 20 lines of the syslog.text file:

```
stream-ServiceEngine# type-tail /local1/syslog.txt 20
Oct 8 21:49:11 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct 8 21:49:11 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct 8 21:49:13 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
```

```
Oct 8 21:49:13 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct 8 21:49:13 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct 8 21:49:15 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct 8 21:49:15 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct 8 21:49:15 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct 8 21:49:17 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct 8 21:49:17 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct 8 21:49:17 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct 8 21:49:19 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct 8 21:49:19 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct 8 21:49:19 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct 8 21:49:21 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct 8 21:49:21 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct 8 21:49:21 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct 8 21:49:23 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct 8 21:49:23 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct 8 21:49:23 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
```

The following example follows the file as it grows:

```
stream-ServiceEngine# type-tail /local1/syslog.txt ?
  <1-65535>  The numbers of lines from end
  follow     Follow the file as it grows
  <cr>
stream-ServiceEngine# type-tail /local1/syslog.txt follow
Oct 8 21:49:39 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct 8 21:49:41 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct 8 21:49:41 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct 8 21:49:41 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct 8 21:49:43 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct 8 21:49:43 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct 8 21:49:43 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct 8 21:49:45 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct 8 21:49:45 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct 8 21:49:45 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct 8 21:49:47 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct 8 21:49:47 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct 8 21:49:47 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct 8 21:49:49 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct 8 21:49:49 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct 8 21:49:49 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
```

undebug

To disable debugging functions, use the **undebug** EXEC command.

undebug *option*

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

We recommend that you use the **debug** and **undebug** commands only at the direction of Cisco Technical Assistance Center (TAC). See the "debug" section on page 2-74 for more information about debug functions.

Valid values for *command* are as follows:

Command	Description	Device Mode
access-lists	Access Control List debug commands.	SE
all	Disables all debugging.	All
authentication	Authentication debug commands.	All
capturecontroller	Capture Controller debug commands.	SE
cdnfs	Debugs the CDS network file system (CDNFS).	SE
cds-origin-manager	CDS Origin Manager debug commands.	
cli	CLI debug commands.	SE
cms	Debugs the centralized management system (CMS).	All
dataserver	Dataserver debug commands.	All
dfs	Distributed filesystem (DFS) debug commands.	SE
dhcp	Dynamic Host Configuration Protocol (DHCP) debug commands.	All
emdb	Embedded database debug commands.	All
http	HTTP debug commands.	SR
logging	LOG debug commands.	All
malloc	Memory allocation debug commands.	All
ntp	Network Time Protocol (NTP) debug commands.	All
rpc	Interbox remote procedure call (RPC) debug commands.	All
service-router	Service Router debug commands.	SE
snmp	Simple Network Management Protocol (SNMP) debug commands.	All

standby	Standby debug commands.	SE
stats	Statistics debug commands.	VOSM
translog	Transaction Log debug commands.	SE, SR
uns	Unified naming service command.	SE
web-engine	Web Engine debug commands.	SE
wi	Web Interface debug commands.	SE

Related Commands

Command	Description
debug	Configures the debugging options.
show debugging	Displays the state of each debugging option.

url-signature

The VDS-OS uses a combination of key owners, key ID numbers, and a word value to generate URL signature keys. To configure the url signature, use the **url-signature** command in global configuration mode.

url-signature key-id-owner *num* **key-id-number** *id_num* {**key** *keyword* | **public key** *url* [**symmetric key** *word* | **private key** *url*]}

no url-signature key-id-owner *num* **key-id-number** *num*

Syntax Description

key-id-owner	Configures the owner ID for this key.
num	Specifies the ID for the owner of this key. The range is from 1 to 32.
key-id-number	Configures the number ID for this key.
id_num	Specifies the ID for the number of this key. The range is from 1 to 16.
key	Configures the encryption key for signing a URL.
keyword	Text of encryption key (maximum of 16 characters, no spaces). **Note** This field accepts only printable ASCII characters (alphabetic, numeric, and others) and does not support a space or the following special characters: pipe (|), question mark (?), double quotes (“), and apostrophe ('). The following special characters are allowed: {}!#$%&()*+,-./;:<=>@\~^[]_.
public-key	Configures the Public Key file location (Privacy Enhanced Mail [PEM]).
url	The URL from where the Public Key file can be downloaded (maximum of 54 characters).
symmetric-key	(Optional) Configure the Symmetric Key.
word	The Symmetric Key (Must be 16 characters, no spaces).
private-Key	(Optional) Configures the Private Key file location (PEM).
url	The URL from where the Private Key file can be downloaded (maximum of 54 characters).

Command Modes

Global configuration (config) mode.

Usage Guidelines

Service Rules for Directing Requests to a Policy Server

If your network is configured to work with Camiant PCMM-compliant third-party policy servers for servicing requests that require guaranteed bandwidth, you can use the following rule patterns and rule actions to filter the requests and to direct them to the policy server. The rule patterns and rule actions also enable you to generate URL signatures in the response for a valid request for a Windows Media metafile (.asx file extension), and to validate the URL signature on incoming requests to the SE. URL signature key authentication is implemented by using the generate-url-signature and validate-url-signature rule actions that can be applied to specific rule patterns.

The following table lists the rule patterns that support the use-icap-service rule action for directing requests that require guaranteed bandwidth to the third-party policy server:

Rule Patern	Description
url-regex	Filters the request based on any regular expression n the URL.
domain	Filters the request based on the domain name specified.
src-ip	Filters the request based on the IP address of the source.
header-field user-agent	Filters the request based on the user agent specified in the request header.
header-field referer	Filters the request based on the referer in the request header.
header-field request-line	Filters the request based on the request line in the request header.

You can set the use-icap-service rule action for any of the rule patterns above. If the request matches the parameters that you have set for the rule pattern, then the SE redirects the request to the third-party policy server using Internet Content Adaptation Protocol (ICAP) services. However, make sure that your network is configured to interoperate with the third-party policy server using ICAP services. You can set up the necessary ICAP configurations from the ICAP Services page. You can also use the rule pattern and rule action to generate URL signatures in the response for a valid request for a Windows Media metafile. You can use the following rule patterns to filter out requests for which you want to generate a URL signature key:

Rule Patern	Description
url-regex	Filters the request based on any regular expression in the URL.
domain	Filters the request based on the domain name specified.

For the rule patterns mentioned above, you can set the following rule actions:

Rule Action	Description
generate-url-signature	Generates the URL signatures in the Windows Media metafile response associated with prepositioned content, based on the SE configuration for the URL signature and this rule action.
validate-url-signature	Validates the URL signature for a request by using the configuration on your SE for the URL signature and allows the request processing to proceed for this request.

Note When configuring service rules, you must configure the same service rules on all SEs participating in a delivery service for the service rules to be fully implemented. The rule action must be common for all client requests because the SR may redirect a client request to any SE in a delivery service depending on threshold conditions.

URL Signing Components

However, because any of these strings in the URL could potentially be edited manually and circumvented by any knowledgeable user, it is important to generate and attach a signature to the URL. This can be achieved by attaching a keyed hash to the URL, using a secret key shared only between the signer (the portal) and the validating component (VDS-OS).

The URL signing script offers three different versions:

- MD5 hash algorithm
- SHA-1 hash algorithm
- SHA-1 hash algorithm with the protocol removed from the beginning of the URL

When a URL is signed for Real-Time Streaming Protocol (RTSP) and a player does a fallback to HTTP for the same URL, the validation fails because the URL signature includes RTSP. If the URL signature does not include the protocol, the fallback URL is validated correctly even though the protocol is HTTP.

If you do not specify a version for the script, MD5 is used and the SIGV string in the script is not added.

At the portal, URLs can be signed for a particular user (client IP address) and expiry time using a URL signing script. The URL signing script example included in this section requires Python 2.3.4 or higher.

Following is an example of the URL signing script using the MD5 security hash algorithm:

```
python vos-ims-urlsign.py http://www.cisco.com/index.html 8.1.0.4 200000 1 2 cisco
```

An example of the resulting signed URL follows:

```
http://www.cisco.com/index.html?IS=0&ET=1241194518&CIP=8.1.0.4&KO=1&KN=2&US=deebacde45bf71
6071c8b2fecaa755b9
```

If you specify Version 1 for the script, SHA-1 is used and the SIGV=1 string is added.

Following is an example of the URL signing script using the SHA-1 security hash algorithm:

```
python vos-ims-urlsign.py http://www.cisco.com/index.html 8.1.0.4 200000 1 2 cisco 1
```

An example of the resulting signed URL follows:

```
http://www.cisco.com/index.html?SIGV=1&IS=0&ET=1241194679&CIP=8.1.0.4&KO=1&KN=2&US=8349348
ffac7987d11203122a98e7e64e410fa18
```

If you specify Version 2 for the script, SHA-1 is used. The protocol from the beginning of the URL is also removed before the signature is generated, and the SIGV=2 string is added. The protocol is RTSP, HTTP, or RTMP. The URL is signed without the protocol, but the final signed URL is printed with the protocol.

Following is an example of the URL signing script using the SHA-1 security hash algorithm with Version 2 specified:

```
python vos-ims-urlsign.py http://www.cisco.com/index.html 8.1.0.4 200000 1 2 cisco 2
```

An example of the resulting signed URL follows:

```
http://www.cisco.com/index.html?SIGV=2&IS=0&ET=1241194783&CIP=8.1.0.4&KO=1&KN=2&US=68b5f5e
d97d1255a0ec42a42a4f779e794df679c
```

Note The URL signature key field accepts only printable ASCII characters (alphabetic, numeric, and others) and does not support a space or the following special characters: pipe (|), question mark (?), double quotes (“), and apostrophe ('). The following special characters are allowed: {}!#$%&()*+,-./;:<=>@\~^[]_

Examples

Following is an example of generating and encrypting the public key and private key using the **url-signature** command:

```
ServiceEngine(config)# url-signature key-id-owner 1 key-id-number 10 public-key
http://1.1.1.1/ec_pub_key private-key http://1.1.1.1/ec_pub_key symmetric-key
```

Following is an example of the URL signing script using the MD5 security hash algorithm:

```
python vos-ims-urlsign.py http://www.cisco.com/index.html 8.1.0.4 200000 1 2 cisco
```

An example of the resulting signed URL follows:

```
http://www.cisco.com/index.html?IS=0&ET=1241194518&CIP=8.1.0.4&KO=1&KN=2&US=deebacde45bf71
6071c8b2fecaa755b9
```

If you specify Version 1 for the script, SHA-1 is used and the SIGV=1 string is added.

Following is an example of the URL signing script using the SHA-1 security hash algorithm:

```
python vos-ims-urlsign.py http://www.cisco.com/index.html 8.1.0.4 200000 1 2 cisco 1
```

An example of the resulting signed URL follows:

```
http://www.cisco.com/index.html?SIGV=1&IS=0&ET=1241194679&CIP=8.1.0.4&KO=1&KN=2&US=8349348
ffac7987d11203122a98e7e64e410fa18
```

If you specify Version 2 for the script, SHA-1 is used. The protocol from the beginning of the URL is also removed before the signature is generated, and the SIGV=2 string is added. The protocol is RTSP, HTTP, or RTMP. The URL is signed without the protocol, but the final signed URL is printed with the protocol.

Following is an example of the URL signing script using the SHA-1 security hash algorithm with Version 2 specified:

```
python vos-ims-urlsign.py http://www.cisco.com/index.html 8.1.0.4 200000 1 2 cisco 2
```

An example of the resulting signed URL follows:

```
http://www.cisco.com/index.html?SIGV=2&IS=0&ET=1241194783&CIP=8.1.0.4&KO=1&KN=2&US=68b5f5e
d97d1255a0ec42a42a4f779e794df679c
```

username

To establish username authentication, use the **username** command in global configuration mode.

username *name* {**cifs-password** | **samba-password**} {**0** *plain_word* | **1** *lan_crypto nt_crypto* | *clear_text*} | **password** {**0** *plain_word* | **1** *crypto_word* | *clear_text*} [**uid** *u_id*] | **privilege** {**0** | **15**}}

no username *name*

Syntax Description

name	Username.
cifs-password	Sets the Windows user password.
samba-password	Deprecated, same as **cifs-password**.
0	Specifies a clear-text password. This is the default password setting.
plain_word	Clear-text user password.
1	Specifies a type 1 encrypted password.
lan_crypto	Encrypted password for LAN Manager networks.
nt_crypto	Encrypted password for Windows NT networks.
clear_text	Unencrypted (clear-text) password for Windows NT networks.
password	Sets the user password.
crypto_word	Encrypted user password.
uid	Sets the user ID for a clear-text password or an encrypted password.
u_id	Encrypted password user ID (the range is 2001 to 65535).
privilege	Sets the user privilege level.
0	Sets the user privilege level for a normal user.
15	Sets the user privilege level for a superuser.

Defaults

The **password** value is set to 0 (cleartext) by default.

Default administrator account:

- **Uid**: 0
- **Username**: admin
- **Password**: default
- **Privilege**: superuser (15)

Command Modes

Global configuration (config) mode.

Usage Guidelines

The **username** command changes the password and privilege level for existing user accounts.

Note The following characters are not permitted in a username or password: ? . / ; [ ] { } “ @ = |.

User Authentication

User access is controlled at the authentication level. For every HTTP or HTTPS request that applies to the administrative interface, including every CLI and API request that arrives at the VDS-OS network devices, the authentication level has visibility into the supplied username and password. Based on CLI-configured parameters, a decision is then made to either accept or reject the request. This decision is made either by checking local authentication or by performing a query against a remote Authentication Server. The authentication level is decoupled from the authorization level, and there is no concept of role or domain at the authentication level.

When local CLI authentication is used, all configured users can be displayed by entering the **show running-config** command. Normally, only administrative users need to have username authentication configured.

Note Every VDS-OS network device should have an administrative password that can override the default password.

User Authorization

Domains and roles are applied by the VOSM at the authorization level. Requests must be accepted by the authentication level before they are considered by the authorization level. The authorization level regulates the access to resources based on the VOSM GUI role and domain configuration.

Regardless of the authentication mechanism, all user authorization configuration is visible in the GUI.

Examples

When you first connect a VDS-OS device to a VDS-OS network, you should immediately change the password for the username *admin*, which has the password *default*, and the privilege-level superuser.

The following example shows how to change the password:

```
ServiceEngine(config)# username admin password yoursecret
```

The following example shows how passwords and privilege levels are reconfigured:

```
ServiceEngine# show user username abeddoe
Uid                 : 2003
Username            : abeddoe
Password            : ghQ.GyGhP96K6
Privilege           : normal user
ServiceEngine# show user username bwhidney
Uid                 : 2002
Username            : bwhidney
Password            : bhlohlbIwAMOk
Privilege           : normal user
ServiceEngine(config)# username bwhidney password 1 victoria
ServiceEngine(config)# username abeddoe privilege 15
User's privilege changed to super user (=15)
ServiceEngine# show user username abeddoe
Uid                 : 2003
Username            : abeddoe
Password            : ghQ.GyGhP96K6
Privilege           : super user

ServiceEngine# show user username bwhidney
Uid                 : 2002
Username            : bwhidney
Password            : mhYWYw.7P1Ld6
Privilege           : normal user
```

Related Commands

Command	Description
show user	Displays the user identification number and username information for a particular user.
show users	Displays the specified users.

vosm

To configure the VDS-OS IP address to be used for the SEs or SRs, or to configure the role and GUI parameters on a VOSM device, use the **vosm** command in global configuration mode. To negate these actions, use the **no** form of this command.

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

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

Syntax Description

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

Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

You can use the **vosm ui port** command to change the VOSM GUI port from the standard number 8443 as follows:

```
VOSM(config)# vosm ui port 35535
```

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

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

After the device is configured with the VOSM 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 VOSM.

Configuring Devices Inside a Network Address Translation (NAT) Firewall

In a VDS-OS network, there are two methods for a device registered with the VOSM (SEs, SRs, or standby VOSM) to obtain configuration information from the primary VOSM. The primary method is for the device to periodically poll the primary VOSM on port 443 to request a configuration update. You cannot configure this port number. The backup method is when the VOSM 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. VDS-OS networks do not work reliably if devices registered with the VOSM are unable to poll the VOSM 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 NAT firewalls. When a device (SEs at the edge of the network, SRs, and primary or standby VOSMs) 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 VOSM. 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 VOSM 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 VOSM's inside local IP address on its NAT, and using this address, rather than the VOSM's inside local IP address, in the **vosm ip** *ip-address* command when you register the device to the VOSM. If the SE or SR is inside a NAT and the VOSM 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 VOSMs

The VDS-OS software implements a standby VOSM. This process allows you to maintain a copy of the VDS-OS network configuration. If the primary VOSM fails, the standby can be used to replace the primary.

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

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

Switching a VOSM from Warm Standby to Primary

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

```
ServiceEngine# configure
ServiceEngine(config)# vosm 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 VOSM. Use the **show cms info** command in EXEC configuration mode 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 VOSM has fully replicated the primary VOSM configuration. If the update time is not current, check whether there is a connectivity problem or if the primary VOSM 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 VOSMs have the same Coordinated Universal Time (UTC) configured.

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

Examples

The following example shows how to configure an IP address and a primary role for a VOSM:

```
VOSM(config)# vosm ip 10.1.1.1
VOSM(config)# vosm role primary
```

The following example shows how to configure a new GUI port to access the VOSM GUI:

```
VOSM(config)# vosm ui port 8550
```

The following example shows how to configure the VOSM as the standby VOSM:

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

The following example shows how to configure the standby VOSM with the IP address of the primary VOSM by using the **vosm ip** *ip-address* command. This command associates the device with the primary VOSM so that it can be approved as a part of the network.

```
VOSM# vosm ip 10.1.1.1
```

web-engine (EXEC configuration)

To configure the Web Engine, use the **web-engine** command in EXEC configuration mode.

web-engine {**debug-module** {**all** | **ContentStore** | **datasource** | **dataxferengine** | **httpcache** | **httpclient** | **httpsessionmgr** | **none**} | **trace-flow** *url* [**add-header** *string*] | **transaction-monitor** {**write-to-file** | *filename*} | **undebug-module** {**datasource** | **dataxferengine** | **httpcache** | **httpclient** | **httpsessionmgr**}

Syntax Description

debug-module	Debugs the specific Web Engine module.
all	Enables debug for all modules.
ContentStore	Content Abstraction Layer (CAL) Content Store module.
datasource	DataSource Module.
dataxferengine	DataXferEngine module.
httpcache	HTTPCache module.
httpclient	HTTPClient module.
httpsessionmgr	HTTPSessionManager module.
none	Disable debug for all modules.
trace-flow	Traces flow of url through the CDN.
url	URL to be in format (http://domain-name/path)
add-header	Additional headers to send along with the request (maximum 3 headers).
string	(Optional) Quoted string of additional header to be in the format header:value.
transaction-monitor	Lists the statistics of the current working.log file. **Note** You must first enable transaction logging to see this command.
write-to-file	(Optional) Writes out the statistics to the file.
filename	Name of the statistics file.
undebug-module	Undebugs the specific Web Engine module.
ContentStore	CAL Content Store module.
datasource	DataSource module.
dataxferengine	DataXferEngine module.
httpcache	HTTPCache module.
httpclient	HTTPClient module.
httpsessionmgr	HTTPSessionManager module.

Defaults

Realtime Monitor interval: 10 seconds

Command Modes

EXEC configuration mode.

Usage Guidelines

See the "web-engine (global configuration)" section on page 2-443 for information on configuring caching parameters.

The **web-engine transaction-monitor** command monitors the transaction logs and publishes the statistics and information regarding latency. For this command to work, transaction logs have to be enabled and must be in apache format or extended squid format. There should be at least one transaction every 10 second, and the output of the command can be logged to a file or printed in the console.

Transaction logs must be enabled to see this command. Enable Transaction logs by entering the **transaction-logs enable** command in global configuration mode.

The logs are written to /local/local1/<*dirname*>. The logs are consumed by a GUI that displays this information as charts. There should be at least one transaction every interval.

Note If the transaction monitor is only run for a short duration, the script is killed before the block has been filled or flushed to a disk, and the output file is empty.

Examples

The following example shows how to debug CAL-related issues:

```
ServiceEngine# debug web-engine trace
ServiceEngine# web-engine debug-module contentStore
ServiceEngine#
```

The following example shows how to debug the DataSource module:

```
ServiceEngine# web-engine debug-module datasource
ServiceEngine#
```

The following example shows how to debug the DataSource module:

```
ServiceEngine# web-engine undebug-module datasource
ServiceEngine#
```

The following example shows how to display the Web Engine statistics without a file name:

```
ServiceEngine# web-engine transaction-monitor
================================================================================
The statistics will be generated every 10 secs if there are any transactions.
Please press Ctrl-C to stop monitoring the transactions logs
==================== Fri Oct 22 13:58:29 UTC 2010 ==================
HTTP Response Code - Statistics
------------------------------
  200  |  404  |

  414  |   44  |
Cache Access Status - Statistics
--------------------------------
TCP_HIT              ==> 414
TCP_MISS             ==> 44
Average Bitrate      ==> 1022.74899 kbps
Longest Latency      ==> 0.06369 secs[http://www.testing.com/index.html]
================================================================================
The statistics will be generated every 10 secs if there are any transactions.
Please press Ctrl-C to stop monitoring the transactions logs
==================== Fri Oct 22 13:58:44 UTC 2010 ==================
HTTP Response Code - Statistics
------------------------------
  200  |  404  |

  606  |   66  |
```

```
Cache Access Status - Statistics
--------------------------------
TCP_HIT              ==> 606
TCP_MISS             ==> 66
Average Bitrate      ==> 1720.00367 kbps
Longest Latency      ==> 0.06369 secs[http://www.testing.com/index.html]
```

The following example shows how to display the Web Engine statistics with a file name:

```
ServiceEngine# web-engine transaction-monitor
================================================================================
The statistics will be generated every 10 secs if there are any transactions.
Please press Ctrl-C to stop monitoring the transactions logs
==================== Mon May 09 06:00:32 PDT 2011 ==================
HTTP Response Code - Statistics
--------------------------------
200  |
 12  |
Cache Access Status - Statistics
--------------------------------
TCP_HIT              ==> 6
TCP_REFRESH_HIT      ==> 1
TCP_MISS             ==> 5
Average Bitrate      ==> 879.26616 kbps
Longest Latency      ==> 0.00627 secs[http://2.225.3.08/index.html]
================================================================================
The statistics will be generated every 10 secs if there are any transactions.

Please press Ctrl-C to stop monitoring the transactions logs
ServiceEngine#
```

The following example shows how to write transaction-monitor logs to an external file and issue a request that the statistics be redirected to the specified file:

```
ServiceEngine# web-engine transaction-monitor write-to-file sree2.txt
================================================================================
The statistics will be generated every 10 secs if there are any transactions.

Please press Ctrl-C to stop monitoring the transactions logs

The Statistics are written to the file /local1/logs/sree2.txt
ServiceEngine#
```

Related Commands

Command	Description
show statistics web-engine	Displays the Web Engine statistics.
show web-engine	Displays the Web Engine information.
web-engine (global configuration)	Configures the Web Engine caching parameters.

web-engine (global configuration)

To configure the Web Engine, use the **web-engine** command in global configuration mode. To negate these actions, use the **no** form of this command.

web-engine {**abr-session-log enable** | **cache** {**age-multiplier** {**days** *num* | **hours** *num* | **minutes** *num* | **seconds** *num*} | **max-ttl** {**days** *num* | **hours** *num* | **minutes** *num* | **seconds** *num*}} | **min-ttl** {**days** *num* | **hours** *num* | **minutes** *num* | **seconds** *num*}} | **http-ingest-logging enable** | **max-concurrent-sessions** *session_num* | **revalidation** {**disable** | **must revalidate**}}

no web-engine {**abr-session-log enable** | **cache** {**age-multiplier** {**days** *num* | **hours** *num* | **minutes** *num* | **seconds** *num*} | **max-ttl** {**days** *num* | **hours** *num* | **minutes** *num* | **seconds** *num*}} | **min-ttl** {**days** *num* | **hours** *num* | **minutes** *num* | **seconds** *num*}} | **http-ingest-logging enable** | **max-concurrent-sessions** *session_num* | **revalidation** {**disable** | **must revalidate**}}

Syntax Description

abr-session-log	Configures ABR session-based transaction logging.
enable	Enables session-based ABR transaction logging.
cache	Configures the Web Engine caching parameters. **Note** The **cache** keyword is not supported in VDS-OS 2.0.
age-multiplier	Expiration time as a percentage of their age.
days	Maximum time to live units, in days.
num	Number of days. The range is form 1 to 1825.
hours	Maximum time to live units, in hours.
num	Number of hours. The range is from 1 to 43800.
minutes	Maximum time to live units, in minutes.
num	Number of minutes. The range is from 1 to 2628000.
seconds	Maximum time to live units, in seconds.
num	Number of seconds. The range is from 1 to 157680000.
max-ttl	Maximum time to live for objects in the cache, in minutes.
min-ttl	Minimum time to live for objects in the cache, in minutes.
http-ingest-logging	Configures http-ingest-logging for each request to Upstream.
enable	Enables http-ingest-logging for each request to Upstream.
max-concurrent-sessions	Configures the maximum concurrent sessions for the Web Engine.
session_num	Maximum number of concurrent sessions for the Web Engine. The range is from 100 to 60000.
revalidation	Enables and disables revalidation requests. **Note** The **revalidation** keyword is not supported in VDS-OS 2.0.
disable	Disables revalidation requests in the Web Engine.
must-revalidate	If **must-revalidate** is configured, all requests are revalidated by the Web Engine.

Defaults

ABR Session Log: disabled
Age Multiplier: 30
min-ttl: 60
max-ttl: 61
Range Cache Fill: disabled
Revalidation: enabled

Command Modes

Global configuration (config) mode.

Usage Guidelines

The **web-engine range-cache-fill** command is not supported in VDS-OS 2.0.

During cache-miss scenarios, the **web-engine range-cache-fill enable** command enables the Web Engine to cache the full content when a client requests a content range where the first byte of the range is zero (0). The full content is cached and only the requested range is sent to the client.

If the first byte of the range is not zero (0), the content is not cached and the client receives only the requested content range from the content origin service.

If this configuration parameter is not enabled and the range request is specified with the first byte of the range being zero and the last byte not specified, the full content is cached on the SE and served to the client.

The request bundling has the following behavior during an active cache-fill session:

- If a content is not cached, the first client accessing that content goes to the origin service to download the full content. This is the cache-fill period.
- During the cache-fill period,
  - If other clients request the same content in a GET of the full object, those clients do not go to the origin service, but feed off of the cache-fill session.
  - If there are clients requesting the same content in a range-request (a portion of the file), those clients go to the origin service directly to fetch that range.

    For small files, when there is a cache-fill in progress that could satisfy the subsequent request, the clients are served the ongoing cache-fill without initiating a range request to the upstream device.

    For large files, if the ongoing cache-fill has not yet been cached, a new feed is immediately initiated for the request range and for subsequent range requests.
- After the object is fully cached, all future requests (both GET and range request) are served from the local cache.

For request bundling, if the range request portion is already cached, it is served out of the local cache, even if the full file is not finished downloading yet. Only when a portion of the range requested is not yet all on disk does the request follow the VDS-OS hierarchy to locate the cached content, ending at the origin service.

The **no web engine range-cache-fill** command does not alter the behavior of the range request "bytes=0-" which caches full content and also serves full content to the client.

The **show running-config** command and the **show web-engine all** command display the configuration state of this parameter.

For dynamic cached contents, the **revalidation** command triggers only after the cached object is expired by the min/max ttl values. The **must-revalidate** command forces the revalidation of cached objects whether or not the cached object is expired.

Note Configuring Web Engine Service Rules is done though the VOSM, not the CLI.

The **web-engine feature-cachefill** command has just one configurable option, **enable**, which turns it on or off.

When the **web-engine abr-session-log enable** command is executed, the Web Engine uses Per Session ABR transaction logs. When it is disabled, the Web Engine uses Per Transaction ABR logs. If ABR session framework is not enabled, the Web Engine uses normal HTTP transaction logs disregarding this configuration. This command is disabled by default.

Ingest Transaction Logs

The **web-engine http-ingest-logging enable** command enables Web Engine ingest transaction logs that are used to log details of every upstream request sent by the Web Engine to the upstream SEs and origin services. Ingest transaction logs only stores request details of cache-miss content and cache-hit content with a revalidation request; details of prefetched content are not stored in the ingest transaction logs.

The Web Engine ingest transaction logs are located in the /local/local1/logs/webengine_ingestlog_clf directory.

The ingest log file format is as follows:

Time URL FailOverSvrList ServerIP BytesRead BytesToRead AssetSize %DownloadComplete DownloadTime(Seconds) ReadCallBack Status-Returned MIME-Type Revalidation-Request VOSDomain ConnectionInfo(LocalPort|ConnectTime|Retry|ReUse) IngestStatus

The following are several ingest log file examples:

```
[26/Aug/2011:04:12:56.429-0700] http://3.1.7.30/error-b404-1170329 3.1.7.35/3.1.7.30/
3.1.7.35 0 0 0 0 6 0 504 - No spirent.spcdn.com 38694|Fri_Aug_26_04:12:56_2011|0|1
READ_TIMEOUT_HEADER

[26/Aug/2011:04:12:55.056-0700] http://3.1.7.30/error-b404-1187409 3.1.7.35/3.1.7.30/
3.1.7.35 0 0 0 0 3 1 500 - No spirent.spcdn.com 38194|Fri_Aug_26_04:12:55_2011|0|1
NO_NEED_TO_GET_BODY

[30/Aug/2011:05:19:02.700-0700] http://os.cdn.we.com/we/test.html 3.1.7.35/7.25.0.20/
3.1.7.35 18028071 18028071 18028071 100 3 1670 200 text/html;charset=UTF-8 No
youtube.cdn.we.com 21449|Tue_Aug_30_05:19:02_2011|0|1 SUCCESS_FINISH

[04/Aug/2011:22:24:11.810-0700] http://7.25.0.20/we/index1.html 7.25.0.20/ 7.25.0.20 0 0 0
0 2 0 504 - Yes[If_None_Match:"5a585a1-19-7a6c8580"] - 20345|Thu_Aug__4_22:24:11_2011|1|1
CONNECT_CB_SOCK_ERR
```

Table 2-74 describes the fields for the ingest transaction log.

Table 2-74 Ingest Transaction Log Fields

Field	Description
Time	Time the request was sent by the Web Engine to the upstream SE or origin service.
URL	Requested URL, including the query string, sent by the Web Engine.

Table 2-74 Ingest Transaction Log Fields (continued)

Field	Description
FailOverSvrList	Hierarchical route look-up information to the upstream SE or origin service. When a cache route look-up is performed for the request, the list of upstream SEs and origin service contacted to fetch the content is included in the log entry.
ServerIP	IP address of the SE or origin service from which the content is downloaded. This is obtained from the FailOverSvrList.
BytesRead	Number of bytes downloaded from the upstream SE or origin service.
BytesToRead	Total number of bytes to be downloaded from the upstream SE or origin service.
AssetSize	Size of the asset (in bytes) requested.
%DownloadComplete	Percentage of asset that has been downloaded to the requesting SE.
DownloadTime (Seconds)	Time to download the incoming stream (in seconds granularity).
ReadCallBack	Number of read call back received to read the response body.
Status-Returned	HTTP status code returned from the upstream SE or origin service.
MIME-Type	MIME type.
Revalidation-Request	Either "Yes" if the request is a revalidation request for a cache hit, or "No" if the request is a cache-miss. If "Yes," the Header-Name:HeaderValue follows. The "If-None-Match" or "If-Not-Modified" headers and their values are included in the log entry.
VOSDomain	This internal header is added by the Web Engine when reaching out to another streamer in the CDN hierarchy. This header value represents the request domain of the end client request.
ConnectionInfo	
LocalPort	Local port used by the streamer to talk to upstream.
ConnectTime	Time at which the connection was established.
Retry	Number of retries on the connection.
Reuse	Number of times the same connection was reused.
IngestStatus	Status of the Ingest. The possible values for this field are: CONNECT_TIMEOUT, CONNECT_CB_SOCK_ERR, CONNECT_SOCK_ERR, CONNECT_TO_SELF, WRITE_READY_TIMEOUT, WRITE_SOCK_ER R_HWEADER, READ_TIMEOUT_HEADER, READ_TIMEOUT_BODY, READ_RCVD_ON_WRITE, READ_SOCK_ERR_HEADER, READ_SOCK_ERR_BODY, HEADER_INVALID_CONT_LEN, HEADER_PARSE_EXCEPTION, HEADER_PARSE_ERR, NO_NEED_TO_GET_BODY, NO_MORE_DATA_TO_READ, HEAD_RESPONSE, SUCCESS_FINISH, INVALID_STATE

Examples

The following example shows how to configure caching parameters:

```
ServiceEngine(config)# web-engine cache min-ttl 20
ServiceEngine(config)#
```

```
ServiceEngine(config)# web-engine cache max-ttl minutes 50
ServiceEngine(config)#
```

Note The **web-engine cache** command is not supported in VDS-OS 2.0.

The following example shows how to enable http ingest logging for each request to Upstream:

```
ServiceEngine(config)# web-engine http-ingest-logging enable
ServiceEngine(config)#
```

The following example shows how to enable cache fill (of full content) on range requests when the first byte is 0(zero):

```
ServiceEngine(config)# web-engine range-cache-fill enable
ServiceEngine(config)#
```

Note The **web-engine range-cache-fill** command is not supported in VDS-OS 2.0.

So the following GET request caches full content (file_cache.html) and serves only 100 bytes (0-99) to the client:

```
GET http://171.79.89.10/file_cache.html HTTP/1.1
Host:171.79.89.10
Range:bytes=0-99
```

But the following GET request does *not* cache the content (here file_no_cache.html) and serves 100 bytes (10-109) to client:

```
GET http://171.79.89.10/file_no_cache.html HTTP/1.1
Host:171.79.89.10
Range:bytes=10-109
```

The following example shows how to disable the cache fill option on range request:

```
ServiceEngine(config)# no web-engine range-cache-fill enable
ServiceEngine(config)#
```

Note The **web-engine range-cache-fill** command is not supported in VDS-OS 2.0.

This GET request does not cache the contents and serves only requested bytes to client(s).

The following example shows how to disable revalidation on the Web Engine:

```
ServiceEngine(config)# web-engine revalidation disable
```

Note The **web-engine revalidation disable** command is not supported in VDS-OS 2.0.

The following example shows how to enable ABR per Session logging:

```
ServiceEngine(config)# transaction-logs enable
ServiceEngine(config)# web-engine abr-session-log enable
```

Or

```
ServiceEngine(config)# transaction-logs enable
```

```
ServiceEngine(config)# web-engine abr-session-log enable exclusive
```

Related Commands

Command	Description
show statistics web-engine	Displays the Web Engine statistics.
show web-engine	Displays the Web Engine information.
web-engine (EXEC)	Configures the Web Engine module.

whoami

To display the username of the current user, use the **whoami** command in EXEC configuration mode.

whoami

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use this command to display the username of the current user.

Examples

The following example shows how to display the username of the user who has logged in to the SE:

```
ServiceEngine# whoami
admin
```

Related Commands

Command	Description
pwd	Displays the present working directory.

write

To save startup configurations, use the **write** command in EXEC configuration mode.

write [**erase | memory | terminal**]

Syntax Description

erase	(Optional) Erases the startup configuration from nonvolatile random-access memory (NVRAM).
memory	(Optional) Writes the configuration to NVRAM. This setting is the default.
terminal	(Optional) Writes the configuration to a terminal session.

Defaults

The configuration is written to NVRAM by default.

Command Modes

EXEC configuration mode.

Usage Guidelines

Use this command to either save running configurations to NVRAM or erase memory configurations. Following a **write erase** command, no configuration is held in memory, and a prompt for configuration specifics occurs after you reboot the SE.

Use the **write terminal** command to display the current running configuration in the terminal session window. The equivalent command is **show running-config**.

The **write memory** command saves modified Websense configuration files (the eimserver.ini, config.xml, and websense.ini files and the Blockpages directory) across disk reconfiguration and VDS-OS software release upgrades.

Note Clicking the **Save Changes** button from the Websense Enterprise Manager window does not save the Websense configuration modifications across device reboots. You need to use the **write memory** command to save the Websense configuration changes across reboots.

Execute the **write memory** command to save the most recent configuration modifications, including websense.ini file modifications and Websense URL filtering configuration changes. The **write memory** command enables the changes made from the external Websense Manager GUI to be saved across disk reconfiguration and upgrades (which might erase disk content).

The Websense configurations from the last use of the **write memory** command are retained under the following situations:

- If the **write memory** command is not used before a reboot but after a disk reconfiguration or a VDS-OS software upgrade that erases disk content.
- If you are using the CLI and did not answer **Yes** when asked if you wanted to save the configurations at the reload prompt.

However, if the **write memory** command has never been used before, then default configurations are applied when the content in the /local1/WebsenseEnterprise/EIM directory on the SE is erased.

Examples

The following command saves the running configuration to NVRAM:

```
ServiceEngine# write memory
```

Related Commands

Command	Description
copy	Copies the configuration or image files to and from the CD-ROM, flash memory, disk, or remote hosts.
show running-config	Displays the current operating configuration.