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.

Command 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, 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
          4096 Sat Feb 12 07:15:23 2005 <DIR>    wmt_vod
```

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.

location community

To configure the community values that are associated with a Proximity Engine, use the **location community** command in BGP configuration (config-bgp) mode. To remove community values that are associated with a Proximity Engine, use the **no** form of this command.

location community *community_string* [**target** *community_string* | **weight** *num*]

no location community *community_string* [**target** *community_string* | **weight** *num*]

Syntax Description

community_string	Community value string associated with the Proximity Engine.
target	(Optional) Specifies the BGP target community.
weight	(Optional) Specifies the location community weight.
num	Location community weight (the range is 1-7).

Command Defaults

By default, no community values are associated with the Proximity Engine.

Command Modes

BGP configuration (config-bgp) mode.

Usage Guidelines

Use the **location community** command to configure community string values. The configuration includes all community values that represent location. When community values are configured, the Proximity Engine creates and maintains a sorted table of communities within BGP.

The maximum number of location communities allowed for each SE is 128.

The *community_string* can be in one of the following forms:

- Community number, such as 100:3535 or 200:4566
- Interval of community numbers, such as 100:3000 to 100:4000 or 100:5000 to 100:6000

Use the **show ip bgp summary** and s**how ip bgp community** commands to display the community values that are configured for a Proximity Engine.

In order for the proximity function to work, one of the following is required:

- Enabled link-state protocol, such as OSPF or IS-IS for IGP proximity.
- Enabled policy routing protocol, such as BGP for best-path proximity, and one of the IGP (OSPF or IS-IS) is required for next hop resolution.

Note All BGP routes must resolve to IGP next hops or directly connected routes.

Previously location-specific communities must be manually configured using the **location community** command. The **location community weight** command includes the weight that must be assigned to the location community. Also in this release, the order the community strings are displayed in the running-config was changed. In the old releases, community strings were displayed in the order of lengths of the strings, but now they are displayed in alphabetical order.

Location community ranges overlaps are not allowed. Specific location communities are always allowed. Thus if location community 5:1-5:10 is already configured, then 5:2-5:3 is not allowed, 5:2-5:7 is also not allowed. 5:5 is allowed:

```
ServiceRouter(config-bgp)# location community 5:1-5:10 weight 2
ServiceRouter(config-bgp)# location community 5:2-5:3
%BGP: Invalid or overlapping location community.
ServiceRouter(config-bgp)# location community 5:2-5:7
%BGP: Invalid or overlapping location community.
ServiceRouter(config-bgp) #location community 5:5
ServiceRouter(config-bgp)#
```

For the proximity calculation, the most specific match's weight is taken. If there is no such match, then the weight of the range is taken. In the example above, a PTA with location-community 5:5, has weight 1 if both PSA and PTA location-community match, and a PTA with location community 5:1 has weight 2, if PSA And PTA location-community also match.

Examples

The following example shows how use the **location community** command to configure community values for a Proximity Engine.

```
ServiceRouter# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ServiceRouter(config)# router bgp 23
ServiceRouter(config-bgp)# location community 100:3535
ServiceRouter(config-bgp)# location community 100:50-100:100
```

The following example shows how to configure the location community weight of 2:

```
ServiceRouter(config)# router bgp 23
ServiceRouter(config-bgp)# location community 5:1-5:10 weight 2
```

The following example associates a source/PSA with a location-community community 1:1 with a target/PTA with a location community 2:2 and the weight of this association is 2. Also, the source and/or target community might be a range:

```
ServiceRouter(config)# router bgp 23
ServiceRouter(config-bgp)# location community 1:1 target 2:2 weight 2
```

The following example associates the source community 1:1 with all target communities in the range 2:0-2:10 with preference weight 2:

```
ServiceRouter(config)# router bgp 23
ServiceRouter(config-bgp)# location community 1:1 target 2:0-2:10 weight 2
```

The following example associates all source communities in the range 1:0-1:10 with target community 2:2 with preference weight 2:

```
ServiceRouter(config)# router bgp 23
ServiceRouter(config-bgp)# location community 1:0-1:10 target 2:2 weight 2
```

The following example associates all source communities in the range 1:0-1:10 with all target communities in the range 2:0-2:10 with preference weight 2. It can also be seen that a PSA with community 1:1 and a PTA with community 2:2 would satisfy all four commands above since 1:1 falls in the range 1:0-1:10 and 2:2 falls in the range 2:0-2:10. In such scenario, where multiple commands satisfy the matching criteria, the weight is based on the preference level of the commands. The preference level of the four commands above is descending in the following order:

1. Specific source community(1:1)-specific target community(2:2)
2. Specific source community(1:1)-range target community(2:0-2:10)

3. Range source community(1:0-1:10)-specific target community(2:2)
4. Range source community(1:0-1:10)-range target community(2:0-2:10)

```
ServiceRouter(config)# router bgp 23
ServiceRouter(config-bgp)# location community 1:0-1:10 target 2:0-2:10 weight 2
```

Related Commands

Command	Description
proximity algorithm bgp location-community	Specifies that the community-based proximity algorithm be used.

log-adjacency-changes

To configure the router to send a syslog message when an IS-IS neighbor goes up or down, use the **log-adjacency-changes** router configuration command. To turn off this function, use the **no** form of this command.

log-adjacency-changes

no log-adjacency-changes

Syntax Description

This command has no arguments or keywords.

Command Defaults

Sending syslog messages when an IS-IS neighbor goes up or down is enabled.

Command Modes

BGP (config-bgp), IS-IS (config-isis) and OSPF configuration (config-ospf) modes.

Usage Guidelines

This command allows you to know about IS-IS neighbors going up or down without turning on the **debug IS-IS adjacency** command. The **log-adjacency-changes** command provides a higher level view of changes in the peer relationship with less output. This command is enabled by default but messages are sent only when up or down (full or down) events are reported.

Examples

The following example shows how to configure the router to send a syslog message when an IS-IS neighbor's state changes:

```
ServiceRouter(config)# router isis
ServiceRouter(config-isis)# log-adjacency-changes
ServiceRouter(config-isis)#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

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.

Command 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 sysfs partition as /local1/syslog.txt. This file contains the output from many of the CDS 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 CDS network, you can use the system message log feature. When a problem occurs in the CDS network, use the system message logs to diagnose and correct such problems.

The syslog.txt file on the CDSM contains information about events that have occurred on the CDSM 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 CDSM because the problem never occurred on the CDSM 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 IDE disk was added. Support for filtering multiple syslog messages for a single failed section for SCSI disks and 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.

log-neighbor-changes

To enable logging of BGP neighbor resets, use the **log-neighbor-changes** BGP configuration command. To disable the logging of BGP neighbor changes, use the **no** form of this command.

log-neighbor-changes

no log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Command Defaults

If the **log-neighbor-changes** command is not issued, neighbor status change messages are not tracked. One exception is a reset, which is always available as output of the **show ip bgp neighbors** command.

Command Modes

BGP configuration (config-bgp) mode.

Usage Guidelines

The **log-neighbor-changes** command enables logging of BGP neighbor status changes (up or down) and resets for troubleshooting network connectivity problems and measuring network stability. Unexpected neighbor resets might indicate high error rates or high packet loss in the network and should be investigated.

Using the **log-neighbor-changes** command to enable status change message logging does not cause a substantial performance impact, unlike, for example, enabling per BGP update debugging.

In order for the proximity function to work, one of the following is required:

- Enabled link-state protocol, such as OSPF or IS-IS for IGP proximity.
- Enabled policy routing protocol, such as BGP for best-path proximity, and one of the IGP (OSPF or IS-IS) is required for next hop resolution.

Note All BGP routes must resolve to IGP next hops or directly connected routes.

Log neighbor changes help keep track of the adjacency changes. Once you enable the **log-neighbor-changes** command, you can monitor BGP logs to see changes and troubleshoot issues by using the **type-tail errorlog/bgp_log.current** command.

Examples

The following example logs neighbor changes for BGP:

```
ServiceRouter(config)# router bgp 23
ServiceRouter(config-bgp)# log-neighbor-changes
ServiceRouter(config-bgp)#
```

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.

Command 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, sysfs name, and long name of the file.
pwd	Displays the present working directory of the SE.

lsp-mtu

To set the maximum transmission unit (MTU) size of IS-IS LSPs, use the **lsp-mtu** IS-IS configuration command. To set the MTU to it's default value, use the **no** form of this command.

lsp-mtu *size*

no lsp-mtu *size*

Syntax Description

size	Maximum number of bytes allowed in LSPs (the range is 128 to 4352).

Command Defaults

The default size is 1497 bytes.

Command Modes

IS-IS configuration (config-isis) mode.

Usage Guidelines

The LSP MTU size describes the amount of information that can be recorded in a single LSP. The **lsp-mtu** command is used to configure the maximum number of bytes allowed in an LSP. If this command is not configured, IS-IS uses the default size of 1500 bytes while sending LSPs for Gigabit Ethernet. Use the **no lsp-mtu** command to configure the maximum number of bytes allowed in an LSP at the default value of 1497 bytes.

Examples

The following example shows how to configure the MTU size to be 1400 bytes.

```
ServiceRouter(config)# router isis
ServiceRouter(config-isis)# lsp-mtu 1400
ServiceRouter(config-isis)# end
ServiceRouter#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies the IS-IS process.

mkdir

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

mkdir *directory*

Syntax Description

directory	Name of the directory to create.

Command 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, 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.

Command 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, 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.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use the **model** command to change the CDE250 model type. Table 2-10 shows the internal and external drives for the CDE250 models.

Table 2-10 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#
```

movie-streamer

To enable and configure the Movie Streamer server, use the **movie-streamer** command in Global configuration mode. To disable the Movie Streamer, use the **no** form of this command.

movie-streamer {**accelerate vod enable | advanced** {**client** {**idle-timeout** *num* **| rtp-timeout**} **| origin server idle-interval** *num*} |**broadcast port-list** *num port_num* **| cache** {**age-multiplier** *num* **| enable | max-ttl** {**days** *num* **| hours** *num* **| minutes** *num* **| seconds** *num*} **| reval-each-request**} **| enable | max-concurrent-sessions** *num* **| proxy outgoing rtsp host** *ip_address port_num* **| transport-src-address** *ip_address*}

no movie streamer {**accelerate vod enable | advanced** {**client** {**idle-timeout** *num* **| rtp-timeout**} **| origin server idle-interval** *num*} **| broadcast port-list** *num port num* **| cache** {**age-multiplier** *num* **| enable | max-ttl** {**days** *num* **| hours** *num* **| minutes** *num* **| seconds** *num*} **| reval-each-request**} **| enable | max-concurrent-sessions** *num* **| proxy outgoing rtsp host** *ip address port num* **| transport-src-address** *ip address*}

Syntax Description

accelerate	Configures Movie Streamer kernel streaming acceleration.
vod	Configures kernel streaming acceleration for VOD.
enable	Enables kernel streaming acceleration.
advanced	Configures Movie Streamer Advanced features.
client	Configures advanced client features.
idle-timeout	Sets the RTSP timeout.
num	Client idle timeout, in seconds. The range is from 0 to 300.
rtp-timeout	Sets the RTP timeout.
origin-server	Configures the advanced origin server.
idle-interval	Sets the origin server idle interval.
num	Server idle interval, in seconds. The range is from 1 to 10.
broadcast	Configures the Movie Streamer live broadcast.
port-list	Specifies a port list.
num	Broadcast list number. The range is from 1 to 1024.
port_num	Broadcast port number.
cache	Configures the Movie Streamer cache.
age-multiplier	Sets the Movie Streamer cache heuristic modifier.
num	Expiration time as a percentage of their age. The range is from 0 to 100.
enable	Enables the Movie Streamer media cache.
max-ttl	Sets the maximum time to live for objects in the cache.
days	Specifies the maximum time to live units, in days.
num	Maximum time to live. The range is from 1 to 1825.
hours	Specifies the maximum time to live units, in hours.
num	Maximum time to live. The range is from 1 to 43800.
minutes	Specifies the maximum time to live units, in minutes.
num	Maximum time to live. The range is from 1 to 2628000.
seconds	Specifies the maximum time to live units, in seconds.

num	Maximum time to live. The range is from 1 to 157680000.
reval-each-request	Sets the scope of revalidation for the request.
enable	Enables the Movie Streamer.
max-concurrent-sessions	Specifies the Movie Streamer maximum concurrent sessions.
num	The maximum concurrent sessions. The range is from 1 to 16000.
proxy	Configures the Movie Streamer proxy.
outgoing	Configures the outgoing proxy.
rtsp	Configures the outgoing RTSP proxy.
host	Specifies the outgoing proxy server.
ip_address	IP address of outgoing proxy server.
port_num	Port number of outgoing proxy server. The range is from 1 to 65535.
transport-src-address	Specifies the source IP address to be set in transport header (useful if behind NAT).
ip_address	Source IP address in transport header.

Command Defaults

days: 1
hours: 72
minutes: 4320
seconds: 259200

Command Modes

Global configuration (config) mode.

Usage Guidelines

The **movie-streamer accelerate vod enable** command enables kernel streaming acceleration for VOD.

The **movie-streamer advanced client** command sets the RTSP or RTP timeout value.

The **movie-streamer advanced origin-server** command sets the origin server idle interval value, which can determine the origin server RTP timeout value.

The Idle Timeout field and the **movie-streamer advanced client idle-timeout** command (as well as the **movie-streamer advanced client rtp-timeout** command), are only intended for performance testing when using certain testing tools that do not have full support of the RTCP receiver report. Setting these timeouts to high values causes inefficient tear-down of client connections when the streaming sessions have ended.

For typical deployments, it is preferable to leave these parameters set to their defaults. The default is 60.

The **movie-streamer advanced client idle-timeout** command has a range from 0 to 300, whereas the Idle Timeout field has a range from 30 to 180. This is by design.

Examples

The following example shows how to set the original server interval:

```
ServiceEngine(config)# movie-streamer advanced origin-server idle-interval 5
```

The following example shows how to set the broadcast port list:

```
ServiceEngine(config)# movie-streamer broadcast port-list 1 5000 5002
```

The following example shows how to set the expiration time as a percentage of the age:

```
ServiceEngine(config)# movie-streamer cache age-multiplier 50
```

The following example shows how to set the content cache maximum TTL:

```
ServiceEngine(config)# movie-streamer cache max-ttl days 100
```

The following example shows how to set the maximum concurrent sessions:

```
ServiceEngine(config)# movie-streamer max-concurrent-sessions 7000
```

The following example shows how to set the outgoing proxy:

```
ServiceEngine(config)# movie-streamer proxy outgoing rtsp host 10.74.61.98 554
```

The following example shows how to set the source IP of the transport header while behind NAT:

```
ServiceEngine(config)# movie-streamer transport-src-address 10.74.61.99
```

The following example shows how to set the client timeout:

```
ServiceEngine(config)# movie-streamer advanced client idle-timeout 150
```

The following example shows how to set the RPT time out:

```
ServiceEngine(config)# movie-streamer advanced client rtp-timeout 150
```

The following example shows how to set the original server interval to 5 second:

```
ServiceEngine(config)# movie-streamer advanced origin-server idle-interval 5
```

The following example shows how to set the broadcast port list:

```
ServiceEngine(config)# movie-streamer broadcast port-list 1 5000 5002
```

The following example shows how to set the Expiration time as a percentage of their age's 50%:

```
ServiceEngine(config)# movie-streamer cache age-multiplier 50
```

The following example shows how to set the cache content max ttl to 100 days:

```
ServiceEngine(config)# movie-streamer cache max-ttl days 100
```

The following example shows how to set the max concurrent sessions to 7000:

```
ServiceEngine(config)# movie-streamer max-concurrent-sessions 7000
```

The following example shows how to set the out going proxy:

```
ServiceEngine(config)# movie-streamer proxy outgoing rtsp host 10.74.61.98 554
```

The following example shows how to set the source the IP of the transport header while behind NAT:

```
ServiceEngine(config)# movie-streamer transport-src-address 10.74.61.99
```

Related Commands

Command	Description
show movie-streamer	Displays the Movie Streamer configuration.
show statistics movie-streamer	Displays statistics for the Movie Streamer.

mtu

To set the interface maximum transmission unit (MTU) packet size, use the **mtu** interface configuration command. Use the **no** form of this command to reset the MTU packet size.

mtu *mtu_size*

no mtu *mtu_size*

Syntax Description

mtu_size	MTU packet size in bytes (576 to 1500).

Command Defaults

The default MTU packet size for an Ethernet interface is 1500 bytes.

Command Modes

Interface configuration (config-if) mode.

Usage Guidelines

The MTU is the largest size of IP datagram that can be transferred using a specific data link connection. Use the **mtu** command to set the maximum packet size in bytes.

Examples

The following example shows how to set the MTU packet size as 1500 bytes:

```
ServiceEngine(config-if)# mtu 1500
```

The following example shows how to reset the MTU packet size:

```
ServiceEngine(config-if)# no mtu 1500
```

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.

multicast (Global Configuration)

To configure multicast client options, use the **multicast** command in Global configuration mode. To disable individual options, use the **no** form of this command.

multicast {**accept-license-agreement** | **back-version-compatibility acns-5-0** | **enable** | **evaluate** | **fixed-carousel enable** | **license-key** *key* | **max-concurrent-jobs** *number_jobs* | **priority-weight** *num* | **sender-delay** *delay*}

no multicast {**accept-license-agreement** | **back-version-compatibility acns-5-0** | **enable** | **evaluate** | **fixed-carousel enable** | **license-key** | **max-concurrent-jobs** | **priority-weight** | **sender-delay**}

Syntax Description

accept-license-agreement	Accepts the multicast client license agreement.
back-version-compatibility	Sets the multicast sender to be compatible with multicast receivers running earlier versions of the Internet Streamer CDS software.
acns-5-0	Specifies that the multicast sender must be compatible with multicast receivers running the ACNS 5.0 software.
enable	Enables the multicast client.
evaluate	Starts or continues the 60-day evaluation period of the multicast client.
fixed-carousel enable	Enable fixed carousel sending, regardless of receiver feedback. The intelligent carousel will be disabled, which does carousel based on receiver feedback. This configuration is applicable only to primary sender and will be removed if this SE is moved to backup sender.
license-key	Requires the license key for the multicast client.
key	Multicast client license key parameters.
max-concurrent-jobs	Specifies the maximum number of jobs that can be scheduled concurrently for multicast distribution.
number_jobs	Maximum number of jobs (1–50). The default is 5.
priority-weight	(Optional) Specifies the percentage of multicast bandwidth that is used for priority-based scheduling.
num	Bandwidth percentage to be used for priority-based scheduling. The range is from 0 to 100.
sender-delay	Sets the multicast sender delay time.
delay	Delay time in seconds (480–7200).

Defaults

Evaluate: 60 days

Sender Delay: 960 seconds.

Maximum Concurrent Jobs: 5

Priority Weight: 50%

Command Modes

Global configuration mode.

Usage Guidelines

In the CDS, content is replicated through a channel distribution architecture. Content in channels can be transmitted by unicast pull, or if multicasting is enabled, by multicast push. Multicasting allows efficient distribution of content to multiple SEs and is useful when many end users are interested in the same content. The Internet Streamer CDS software supports Pragmatic General Multicast (PGM)-based multicast replication using either satellite or multicast-enabled terrestrial infrastructures.

Multicast delivery enables the distribution of streaming media by allowing different receiving devices on the IP multicast to receive a single stream of media content from the SE simultaneously. This method can save significant network bandwidth consumption, because a single stream is sent to many devices, rather than sending a single stream to a single device every time that this stream is requested.

This multicast delivery feature is enabled by setting up a multicast address on the SE to which different devices, configured to receive content from the same channel, can subscribe. The delivering device sends content to the multicast address set up at the SE, from which it becomes available to all subscribed receiving devices.

To take advantage of multicasting, all devices, including SEs, routers, and clients, must be multicast enabled. For this reason, multicasting is mostly used in local networks where routers can be configured for multicasting. Multicast delivery over the Internet can only be accomplished when all the devices that participate in the multicast have been enabled for multicasting.

For multicast content replication, SEs are grouped into multicast clouds. A multicast cloud consists of one sender SE, an optional backup sender SE, and at least one receiver SE in a hub and spoke topology. All the SEs in one multicast cloud share a unique advertisement address that allows them to communicate multicast session information. The multicast cloud is then associated with one or more multicast-enabled channels.

In pull-based unicast content distribution, a unicast receiver pulls file data out of the proper forwarder (or root SE) when a client requests the content. In multicast content distribution, the sender SE in a multicast cloud proactively pushes content into the cloud according to a preconfigured schedule.

The receiver SEs listen on the advertisement IP address for information on the content to be replicated from the sender and decide whether to accept an advertisement and whether to receive the content.

The content metadata (machine-readable information that describes the characteristics of the content) must be distributed to a receiver first before the content can be replicated. The content metadata helps to define what content to retrieve, how the content will be retrieved, how recently the content has been updated, how the content is to be pre-positioned (for example, the expiration time), and so forth. The metadata is always distributed using unicast. The content, however, can be replicated using either multicast or unicast. A multicast receiver rejects the multicast sender's advertisement of a file if the proper content metadata has not arrived. During the content distribution process, both the content and its associated information describing the content, called the metadata, are distributed. A multicast receiver does not accept any multicast content unless it has already received the associated metadata for that particular content.

Use the **multicast fixed-carousel enable** command to enable fixed-carousel sending. Carousel sending, which refers to the multicast retransmission of content, allows receivers who join a multicast group after a distribution has ended or who miss some content to receive the content without requiring a unicast transmission. By default, the SE uses intelligent carousel sending, which means that the retransmission is guided by feedback from the content receivers. Late-joining receivers or receivers that missed some content send a negative acknowledgement (NACK) to the sender for any files that were not received.

Fixed-carousel sending causes the content to be sent without depending on any receiver feedback. When this feature is enabled, the SE continuously retransmits the content after waiting for the time specified by the **sender-delay** option. You can use the **fixed-carousel** option when sending the content to receivers using a release of the Internet Streamer CDS software Release 3.0 or later, which do not send NACKs to

the sender. This configuration is allowed only for the primary sender and is not supported for an SE configured as a backup sender. Use the **no multicast fixed-carousel enable** command to disable fixed-carousel sending and to restore the default configuration.

Use the **multicast max-concurrent-jobs** command option to set the maximum number of objects that can be scheduled concurrently for multicast distribution. When networks are reliable or the size of files being multicast is small, we recommend that you set the maximum number of concurrent objects to 50. However, when networks are unreliable or the size of files being multicast is large, a smaller number of concurrent objects (for example, five) is recommended. The default maximum number of jobs is five.

The **priority-weight** option allows you to change the percentage of multicast bandwidth that is used for priority-based scheduling. By default, 50 percent of the bandwidth is allocated for a priority-based queue and 50 percent is allocated for a time-based, first in, first out (FIFO) queue. The time-based queue allows the system to process lower-priority traffic in a timely way even when it frequently receives large, high-priority requests.

Multicast Sender Delay

The multicast sender delay interval is the amount of time before each multicast transmission begins. A period of delay before the actual multicast transmission begins is required to allow the content metadata time to propagate to the receiver SE. The metadata contains the content file and configuration information that is necessary for the successful transmission of content files. The sender delay parameter is used to configure an extra delay before a multicast transmission can begin.

When configuring the sender delay interval, you must take into account that the content metadata must first propagate to the receiver before the multicast transmission can begin. During a multicast session, a receiver SE sends out periodic requests for files that it has not received. The sender retransmits files only as requested by the receiver SE. A multicast receiver will reject a multicast sender's advertisement of a file if the associated content metadata has not arrived. The sender delay option allows you to configure enough time for the metadata to propagate to the receiver, and avoid having the receiver reject the multicast sender's advertisement of a file.

To configure the sender delay interval, use the multicast sender-delay global configuration command on a sender SE. The **sender-delay** option controls the length of time that the multicast sender must wait for its associated metadata to propagate to the multicast receivers. The default delay time value is 960 seconds, the minimum is 480 seconds, and the maximum is 7200 seconds. You can configure the duration of the delay based on your expectation or best guess of the amount of time required for the metadata to be propagated. The system takes this user-configured sender delay value and delays the multicast transmission for a period defined by the sender delay.

Note The sender delay interval cannot be configured using the CDSM GUI. You must configure the sender delay interval using the CLI of the sender SE.

Multicast License Key

Before you can create a multicast cloud, you must have a multicast distribution license key (purchased from Cisco Systems) and SEs that are enabled for multicasting. These multicast-enabled SEs can then be assigned as sender and receiver SEs when you configure the multicast cloud.

SEs for multicasting must be assigned to the multicast cloud, which in turn is assigned to multicast-enabled channels. Also, you need to assign individual SE senders and receivers of the cloud to the particular multicast-enabled channel. You must do this additional step even though the multicast cloud is associated with the channel.

Note You must assign the multicast cloud to a channel first, and then assign the individual SEs to the channel.

Use the **no multicast license-key** command to uninstall a license key if it is no longer needed on the device because the multicast licensed product feature is not needed. After you uninstall a license key on one device, you can use the key on another device if that device supports the multicast license key.

Note You must disable the multicast feature using the **no multicast enable** command before you uninstall the multicast license key.

Examples

The following example shows how to accept the multicast distribution license for an SE:

```
ServiceEngine# configure
ServiceEngine(config)# multicast accept-license-agreement
```

The following example shows how to enter the multicast distribution license key for an SE:

```
ServiceEngine(config)# multicast license-key 123456789
```

The following example shows how to enable multicasting on an SE:

```
ServiceEngine(config)# multicast enable
```

Related Commands

Command	Description
multicast (EXEC configuration	Generates multicast packets and test connectivity through multicast routers.
show multicast	Displays the multicast end-user license agreement.

multicast (EXEC Configuration)

To generate multicast packets and test connectivity through multicast routers, use the **multicast** command in EXEC configuration mode.

multicast connectivity-test {**cloud-id** *cloud_id* [**duration** *duration_num* [**message-length** | **mullticast-address** *multicast_addr* | **output-style** {**detail** | **error**} | **port** *port_num*] | **packet-count** *packet_num*] | **cloud-name** *name* [**duration** *duration* [**message-length** | **multicast-address** *multicast_addr* | **output-style** {**detail** | **error**} | **port** *port_num*] | **packet-count** *packet_num*] | **receive** *multicast_ip_addr* **interface** *interface_ip_addr* | s**end** *multicast_ip_addr ttl* **interface** *interface_ip_addr* | **streamer** *receiver_ip_addr* {*receiver_ip_addr* | **multicast-address** *multicast_addr* [**duration** *duration* [**FEC-size** *size* | **max-transfer-rate** *rate* | **message-length** | **output-style** {**detail** | **error**} | **port** *port_num*] | **packet-count** *packet_num* | **time-to-live** *ttl*]}}

Syntax Description

connectivity-test	Verifies multicast connectivity between a sender and multiple receivers.
cloud-id	Sends Pragmatic General Multicast (PGM) packets to the multicast cloud.
cloud_id	Cloud ID. The range is from 0 to 4294967295.
duration	(Optional) Configures the length of time over which PGM packets are to be sent to receiver SEs. This is the default option for **multicast-address**.
duration	Number of seconds that PGM packets are sent to receiver SEs. The range is from 30 to 3600; suggested number is 180.
message-length	(Optional) Message length to send.
multicast-address	(Optional) Configures the multicast IP address to be used for sending PGM packets. When you use the **cloud-id** or **cloud-name** option, you can choose not to specify the multicast address. When the multicast address is not specified, the advertising IP address specified in the multicast cloud configuration is used as the multicast address.
multicast_addr	Multicast Address to use for generating PGM Packets.
output-style	(Optional) Define the output display style.
detail	Prints the Detailed Report.
error	Prints the Error Report.
port	(Optional) Destination port to send packets.
port_num	Destination port to send packets. Range is 1025 to 65535; suggested amount is 7000.
packet-count	(Optional) Configures the number of PGM packets to be sent to receiver SEs.
packet_num	Number of PGM packets to send each receiver SE. The range is from 50 to 4096; suggested number is 100.
cloud-name	Sends PGM packets to the multicast cloud.
cloud-name	Name of the cloud.
receive	Receives PGM packets from the multicast address.
multicast_ip_addr	Multicast IP address to listen for PGM Packets.
interface	Interface to be used for Multicast.
interfrace_ip_addr	Interface IP address.

send	Sends PGM packets to the multicast address.
ttl	Time to Live for the multicast packet. Range is from 1 to 255; suggested is 255.
streamer	Sends PGM packets to receiver SEs.
receiver_ip_addr	IP Address of the Receiver SE (max up to 20 Receivers) to check the multicast connectivity.
FEC-size	(Optional) Configures the appending of forward error correction (FEC) redundancy bytes.
size	Number of FEC redundancy bytes to be appended (8–128). The values must be powers of 2 (for example, 8, 16, 32, or 64). The default is 8.
max-transfer-rate	(Optional) Configures the maximum bandwidth that can be used for this multicast transmission.
rate	Maximum Transfer Rate to generate PGM Packets. The range is from 56 to 1000000; suggested is 128Kb.
time-to-live	(Optional) Configures the maximum number of hops permitted for PGM packets before they expire on the network. For each hop, the original specified TTL is decremented by 1. When the TTL reaches 0, PGM packets expire and are no longer forwarded through the network.

Command Defaults

Duration: 180 seconds

Packet Count: 100

FEC Size: 8

Maximum Transfer Rate: 128 kbps

Port: 7000

Time-to-live: 255

Message Length: 1024

Output Style: Detail Report

Command Modes

EXEC configuration mode.

Usage Guidelines

You can use the **multicast connectivity-test** command to test multicast connectivity within the CDS network. The **multicast connectivity-test** command options run pgmrategen (the PGM packet generation application) and pgmratemon (the PGM packet receiver application) in the background to test multicast connectivity. These applications use the PGM protocol, which allows a receiver to report lost data and to request retransmission from the sender. With PGM, the sender multicasts sequenced data packets, and the receivers reply with unicast negative acknowledgments (NACKs) when data packets are missing from the expected sequence. Network elements forward the NACKs to the multicast sender and confirm each hop by multicasting a NACK confirmation on the interface on which the NACK was received.

Multicast Forward Error Correction

Forward error correction (FEC) is a type of data encoding that protects transmissions against errors, without requiring retransmission. The FEC number denotes the number of packets that will be encoded into one FEC transmission group. A higher FEC number means that the transmission group size is larger. The multicast may be more error-resistant, but there will also be more computational overhead on the multicast sender and receivers. No bandwidth overhead is related to FEC.

In the Internet Streamer CDS 3.0 software, the FEC default value is 8. If the multicast sender device is a high-end SE model, you can set this number higher to improve multicast reliability when your network connectivity has a high uniform loss rate. However, we do not recommend that you set this number beyond 64, because it may place too much of a load on all the receiver SEs.

You can also set proactive FEC using the PGM configuration file (a text file accessible from the SE CLI in the /local1/multicast-expert-config/ directory). Proactive FEC is the number of extra packets that the multicast sender proactively sends out for every FEC number of data packets. The proactive FEC default value is 0. You can set the proactive FEC number higher for better multicast reliability. For example, you can set 2 proactive packets for every 16 FEC packets at the expense of 12.5 percent traffic overhead (2 divided by 16).

Proactive FEC is an additional reliability measure above and beyond that of normal FEC. Although normal FEC does not incur bandwidth overhead, proactive FEC does use bandwidth overhead. Proactive FEC primarily protects the multicast from uniform losses. For example, if the network has a uniform loss rate of 15 percent, then a proactive FEC of 2 extra packets for every 16 FEC packets (a 12.5 percent bandwidth overhead) cuts the effective loss rate down to 2.5 percent. Most network losses are not completely uniform. Still, during bursts, proactive FEC undercuts the effective burst loss rate. For example, if the burst loss rate is 20 percent while the average loss rate is 2 percent, with proactive FEC at 12.5 percent, the receiver SEs experience a burst loss rate of 7.5 percent and an average loss rate near 0 percent.

Testing Multicast Connectivity in CDS Networks

The **multicast connectivity-test** command options allow you to test multicast connectivity in the CDS networks. You can specify a maximum of 20 multicast receiver SEs using this option. Use the **cloud-id** or **cloud-name** options to test multicast connectivity to receiver SEs grouped into multicast clouds in the CDS network. There is no limit to the number of SEs you can have in a multicast cloud.

The **cloud-id** or **cloud-name** options initiate the following sequence of events:

1. When you specify the IP addresses of the receiver SEs, multicast cloud ID, or multicast cloud name, you initiate the multicast connectivity test.
2. The multicast sender initiates RPC calls to the receiver SEs, which prompt them to listen for the PGM multicast data on the default port or the port specified in the **multicast connectivity-test** command.
3. The SE displays the following:
   - A list of receiver SEs that failed to respond to the RPC calls
   - Warning messages if multicast is not enabled on any receiver SE
4. The multicast sender starts sending PGM packets to the specified multicast address. The receiver SE keeps updating the session statistics for each packet received.

   If you interrupt the test by pressing **Ctrl-C**, the multicast sender sends a notification to all receiver SEs to stop listening and displays the information obtained so far.
5. After the multicast session is completed or the transmission has timed out, the receiver SE sends the statistics to the multicast sender using an RPC call.

Note If the multicast receiver SE times out, it sends a "no packet received" error message to the multicast sender if it has not received any PGM packets for 60 seconds. Similarly, the multicast sender waits for 60 seconds for a response from the receiver SE before timing out.

6. The multicast sender displays the statistics obtained for the session.
7. The multicast sender repeats the test with the receiver SEs and generates a consolidated report.

Using the cloud-id or cloud-name Option

You can use the **cloud-id** or **cloud-name** options to test multicast connectivity in large networks where a number of SEs are grouped under multicast clouds.

Note You cannot specify values for the optional parameters **FEC-size** and **max-transfer-rate** when the **cloud-id** or **cloud-name** options are used. The values for these two parameters are taken from the multicast cloud configuration.

Use the **multicast connectivity-test cloud-name** command to test the multicast connectivity to the receiver SEs in the multicast cloud mcloud1.

The multicast address is not specified in this example. The Internet Streamer CDS software uses the advertisement IP address specified in the multicast cloud configuration as the multicast address. Because no values were specified for the options, the Internet Streamer CDS software uses the default values for all the optional parameters.

multicast connectivity-test send Command

To test the multicast connectivity to the receiver SEs listening to a specific multicast address, use the **multicast connectivity-test send** command. This command runs the pgmrategen application, which continuously sends PGM packets to the specified multicast IP address. After you enter this command, the system displays the percentage of packets that have been multicast and stops sending packets when the packets sent reaches 100 percent. Press **Ctrl-C** to interrupt the PGM application and return to the EXEC prompt.

To determine the number of network elements through which the packet can pass before reaching the receiver, specify the Time To Live (TTL), which can vary between 1 and 255.

multicast connectivity-test receive Command

To receive PGM packets, use the **multicast connectivity-test receive** command. Entering this command runs the pgmratemon application, which listens for the PGM multicast data transmitted from a PGM sender on the specified multicast IP address. When a packet is received, the pgrmratemon application lists the packet size and bandwidth.

To test the multicast connectivity between two SEs, use the same multicast IP address for both send and receive. The pgmratemon application terminates by itself after a default period of 3 minutes and returns to the EXEC prompt. You can press **Ctrl-C** to terminate the pgmratemon application and return to the EXEC prompt.

Examples

The following example shows the output of the **multicast connectivity-test** command for a multicast IP address of 239.1.1.1 and receiver SE IP addresses 10.43.27.2 and 10.43.27.4:

```
ServiceEngine# multicast connectivity-test 10.43.27.2 10.43.27.4 multicast-address
239.1.1.1
```

```
Connecting to Receiver : 10.43.27.2
Starting PGM Receiver on the SE 10.43.27.2
Connecting to Receiver : 10.43.27.4
Starting PGM Receiver on the SE 10.43.27.4
Packet Generation thread has started. It will start sending packets after PGMReceivers
have been started
Time Elapsed : 180 seconds
PGM Sender has finished sending packets. Awaiting Receiver response
Will wait for 60 seconds...

Configuration
-------------
Multicast Address : 239.1.1.1
Port : 7000
Max Rate to send PGM Packets : 128 kbps
Time to live for multicast packets : 255
Forwarder Error Correction Size : 8

Detailed Report
----------------

Receiver IP : 10.43.27.2
Duration : 180 seconds
No of Packets received : 1134
Packet Length : 1024 Bytes
Minimum BW : 5.714 KBps
Maximum BW : 7 KBps
Average BW : 6.291 KBps
NAK Count : 0

Receiver IP : 10.43.27.4
Duration : 180 seconds
No of Packets received : 1134
Packet Length : 1024 Bytes
Minimum BW : 5.691 KBps
Maximum BW : 7 KBps
Average BW : 6.298 KBps
NAK Count : 0

Summary Report
--------------
Total number of receivers : 2
No: of receivers which received Packets : 2
No: of receivers which did not receive Packets : 0
No: of RPC calls failures : 0
No: of Other Errors obtained from Receivers : 0
```

The following example shows all the optional parameters and default values:

```
ServiceEngine# multicast connectivity-test 10.77.155.171 10.77.155.175 10.77.155.179
multicast-address 239.10.1.11 duration 180 FEC-size 8 max-transfer-rate 128
message-length 1024 output-style detail port 7000 time-to-live 255
```

The following example shows the **multicast connectivity-test cloud-name command** with all the optional parameters and default values:

```
ServiceEngine# multicast connectivity-test cloud-name mcloud1 duration 180 message-length
1024 output-style detail port 7000
```

The following example shows the output of the **multicast connectivity-test cloud-name** command for the multicast cloud Mcloud1. Because the multicast address was not specified, the Internet Streamer CDS software uses the advertisement IP address 239.1.1.1, specified in the multicast cloud configuration, as the multicast IP address. PGM packets are sent to the two receiver SEs (IP addresses 10.43.27.2 and 10.43.27.4) that make up the multicast cloud Mcloud1.

```
ServiceEngine# multicast connectivity-test cloud-name Mcloud1
Connecting to Receiver : 10.43.27.2
Starting PGM Receiver on the SE 10.43.27.2
Connecting to Receiver : 10.43.27.4
Starting PGM Receiver on the SE 10.43.27.4
Packet Generation thread has started. It will start sending packets after PGMReceivers
have been started
Time Elapsed : 180 seconds
PGM Sender has finished sending packets. Awaiting Receiver response
Will wait for 60 seconds...

Configuration
-------------
Multicast Address : 239.1.1.1
Port : 7000
Max Rate to send PGM Packets : 10000 kbps
Time to live for multicast packets : 255
Forwarder Error Correction Size : 16

Detailed Report
----------------

Receiver IP : 10.43.27.4
Duration : 180 seconds
No of Packets received : 1139
Packet Length : 1024 Bytes
Minimum BW : 4.903 KBps
Maximum BW : 7 KBps
Average BW : 6.296 KBps
NAK Count : 0

Receiver IP : 10.43.27.2
Duration : 180 seconds
No of Packets received : 1139
Packet Length : 1024 Bytes
Minimum BW : 5.641 KBps
Maximum BW : 7 KBps
Average BW : 6.319 KBps
NAK Count : 0

Summary Report
--------------
Total number of receivers : 2
No: of receivers which received Packets : 2
No: of receivers which did not receive Packets : 0
No: of RPC calls failures : 0
No: of Other Errors obtained from Receivers : 0
```

The following example shows the output of the **multicast connectivity-test send** command for a multicast IP address of 239.1.1.1 and TTL of 255:

```
ServiceEngine# multicast connectivity-test send 239.1.1.1 255
Starting pgmrategen ....
pgmrategen is already running.  Exiting previous instance
Sending 1024 messages of 1024 bytes (1024 Kbytes)
PGM rate is 1024 Kbps
Progress: 99%
```

```
Total time 159.924 seconds, 6.40302 KBps, 52.4536 Kbps
```

The following example shows the output of the **multicast connectivity-test receive** command:

```
ServiceEngine# multicast connectivity-test receive 239.1.1.1
Starting pgmratemon ....
This SE is not configured as Multicast receiver in any cloud
Configuring this SE as Satellite mode receiver

Press ^C to abort or wait for 3 mins to exit....

Multicasting PGM multicast data to SmartPGM receivers on multicast address 239.1

Sending 1024 messages of 1024 bytes (1024 Kbytes)
PGM rate is 1024 Kbps
Progress: 99%
Total time 8.39756 seconds, 121.94 KBps, 998.934 Kbps

Exiting....
Stopping pgmratemon
ServiceEngine#
```

Related Commands

Command	Description
multicast (Global configuration)	Configure multicast client options.
show multicast	Displays the multicast end-user license agreement.

neighbor

To configure BGP neighbors, use the **neighbor** BGP configuration command. To return to the default, use the **no** form of this command.

neighbor *ip_address* {**ebgp-multihop** *TTL* | **password** *word* | **remote-as** *as_number* | **timers** *keepalive_timer hold_timer*}

no *ip_address* {**ebgp-multihop** *TTL* | **password** *word* | **remote-as** *as_number* | **timers** *keepalive_timer hold_timer*}

Syntax Description

ip_address	IP address of the neighbor.
ebgp-multihop	Sets the Time-to-Live (TTL) value for the EBGP multihop scenarios.
TTL	Time-to-Live value. The range is from 1 to 255.
password	Specifies the BGP neighbor password.
word	BGP MD5 password.
remote-as	Specifies the Remote Autonomous Systems (AS) number.
as_number	Autonomous system to which the neighbor belongs.
timers	Configures keepalive and hold timers.
keepalive_timer	Keepalive timer interval, in seconds. The range is from 0 to 3600.
hold_timer	Hold timer interval, in seconds. The range is from 0 to 3600.

Command Defaults

- There are no BGP or multi protocol BGP neighbor peers.
- Default TTL value is 1 for all neighbors.
- Keepalive timer interval is set to 60 seconds, and the hold timer interval is set to 180 seconds.

Command Modes

BGP configuration (config-bgp) mode.

Usage Guidelines

Use the **neighbor ebgp-multihop** BGP configuration command to set the TTL value for the EBGP multihop scenarios.

Specifying a neighbor with an autonomous system number that matches the autonomous system number specified in the **router bgp** Global configuration command identifies the neighbor as internal to the local autonomous system. Otherwise, the neighbor is considered as external.

Use the **neighbor remote-as** command to add a neighbor to the BGP, or multi protocol BGP table, before setting the TTL value for the neighbor.

By default, neighbors that are defined using the **neighbor remote-as** command in router configuration mode exchange only unicast address prefixes.

Use the **neighbor remote-as** command before setting the TTL value.

In order for the proximity function to work, one of the following is required:

- Enabled link-state protocol, such as OSPF or IS-IS for IGP proximity.
- Enabled policy routing protocol, such as BGP for best-path proximity, and one of the IGP (OSPF or IS-IS) is required for next hop resolution.

Note All BGP routes must resolve to IGP next hops or directly connected routes.

Examples

The following example shows that a router at the address 192.168.86.3 is a neighbor in autonomous system number 23, and has a ebgp-multihop TTL value of 3:

```
ServiceRouter(config)# router bgp 23
ServiceRouter(config-bgp)# neighbor 192.168.86.3 remote-as 23
ServiceRouter(config-bgp)# neighbor 192.168.86.3 ebgp-multihop 3
ServiceRouter(config-bgp)#
```

The following example shows how to specify that a router at the address 192.168.86.3 is a neighbor in autonomous system number 23:

```
ServiceRouter(config)# router bgp 23
ServiceRouter(config-bgp)# neighbor 192.168.86.3 remote-as 23
ServiceRouter(config-bgp)#
```

The following example shows that a router at the address 192.168.86.3 is a neighbor in autonomous system number 23, and its keepalive timer interval and hold timer interval are set to be 100 seconds and 200 seconds, respectively.

```
ServiceRouter(config)# router bgp 23
ServiceRouter(config-bgp)# neighbor 192.168.86.3 remote-as 23
ServiceRouter(config-bgp)# neighbor 192.168.86.3 timers 100 200
ServiceRouter(config-bgp)#
```

To confirm that timers are updated correctly, use the **show ip bgp neighbors** command. The following example output shows that the keepalive interval has been changed to 100 seconds and the hold timer has been changed to 200 seconds:

```
ServiceRouter> show ip bgp neighbors

BGP neighbor is 192.168.86.3, remote AS 23, ibgp link, Peer index 1
  BGP version 4, remote router ID 192.168.86.3
  BGP state = Established, up for 1d05h
  Peer is directly attached, interface GigabitEthernet 2/0
  Last read 0.868226, hold time = 200, keepalive interval is 100 seconds
  Last written 00:00:09, keepalive timer expiry due 00:01:30
  Received 78444 messages, 0 notifications, 0 bytes in queue
  Sent 1788 messages, 0 notifications, 0 bytes in queue
  Connections established 1; dropped 0
  Last reset by us never, due to process restart
  Last reset by peer never, due to process restart
  Neighbor capabilities:
  Dynamic capability: advertised (mp, refresh, gr)
  Dynamic capability (old): advertised
  Route refresh capability (new): advertised received
  Route refresh capability (old): advertised received
  Address family IPv4 Unicast: advertised received
  For address family: IPv4 Unicast
  BGP table version 1, neighbor version 810749
  8518 accepted paths consume 613296 bytes of memory
```

```
  0 sent paths
  Local host: 192.168.86.47, Local port: 58920
  Foreign host: 192.168.86.3, Foreign port: 179
  fd = 35

ServiceRouter>
```

Related Commands

Command	Description
router bgp	Configures a BGP routing process.

net

To configure an IS-IS network entity title (NET) for a Connectionless Network Service (CLNS) routing process, use the **net** IS-IS configuration command. To remove a NET, use the **no** form of this command.

net *network_entity_title*

no net *network_entity_title*

Syntax Description

network_entity_title	NET that specifies the area address and the system ID for a CLNS routing process. Either an address or a name may be specified.

Command Defaults

No *NET* is configured and the CLNS process does not start without a NET.

Command Modes

IS-IS configuration (config-isis) mode.

Usage Guidelines

Under most circumstances, one and only one NET must be configured.

A NET is a network service access point (NSAP) where the last byte is always zero. On a Proximity Engine running IS-IS, a NET can be 8 to 20 bytes. The last byte is always the n-selector and must be zero.

The six bytes directly in front of the n-selector are the system ID. The system ID length is a fixed size and cannot be changed. The system ID must be unique throughout each area (Level 1) and throughout the backbone (Level 2).

All bytes in front of the system ID are the area ID.

Even when IS-IS is used to perform IP routing only (that is, no CLNS routing enabled), a NET must still be configured to define the router system ID and area ID.

- Area ID must match the area ID of the IS-IS router that the Proximity Engine is pairing with.
- System ID is unique for each Proximity Engine.

Examples

The following example shows how to use the **net** command to configure a router with system ID 0001.0c11.1111.00 and area ID 47.0004.004d.0001:

```
ServiceRouter(config)# router isis
ServiceRouter(config-isis)# net 47.0004.004d.0001.0001.0c11.1111.00
ServiceRouter(config-isis)#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

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 Defaults

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 Defaults

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.

network area

To define the interfaces on which OSPF runs and the area ID for those interfaces, use the **network area** router configuration command. To disable OSPF routing for interfaces defined with the address wildcard-mask pair, use the no form of this command.

network *ip_address wildcard_mask* **area** *area_id*

no network *ip_address wildcard_mask* **area** *area_id*

Syntax Description

ip_address	IP address in the form of *xxx.xxx.xxx.xxx*
wildcard_mask	IP-address-type mask that includes “don’t care” bits.
area_id	Area that is to be associated with the OSPF address range. It can be specified as either a decimal value or as an IP address. If you intend to associate areas with IP subnets, you can specify a subnet address as the value of the *area_id.*

Note Any individual interface can only be attached to a single area. If the address ranges specified for different areas overlap, the software adopts the first area in the network command list and ignore the subsequent overlapping portions. In general, it is recommend that you configure address ranges that do not overlap to avoid inadvertent conflicts.

Command Defaults

OSPF routing for interfaces is disabled by default.

Command Modes

OSPF configuration (config-ospf) mode.

Usage Guidelines

The *ip_address* and *wildcard_mask* arguments together allow you to define one or multiple interfaces to be associated with a specific OSPF area using a single command. Using the *wildcard_mask* argument allows you to define one or multiple interfaces to be associated with a specific OSPF area using a single command. If you intend to associate areas with IP subnets, you can specify a subnet address as the value of the *area_id* argument.

For OSPF to operate on the interface, the primary address of the interface must be covered by the **network area** command. If the **network area** command covers only the secondary address, it does not enable OSPF over that interface.

The Proximity Engine sequentially evaluates the *ip_address wildcard_mask* pair for each interface as follows:

1. The *wildcard_mask* is logically ORed with the interface IP address.

2. The *wildcard_mask* is logically ORed with the *ip_address* argument in the **network** command.

3. The software compares the two resulting values. If they match, OSPF is enabled on the associated interface and this interface is attached to the OSPF area specified.

There is no limit to the number of **network area** commands that can be used on the router.

Note Any individual interface can only be attached to a single area. If the address ranges specified for different areas overlap, the software adopts the first area in the network command list and ignores the subsequent overlapping portions. In general, we recommend that you configure address ranges that do not overlap to avoid inadvertent conflicts.

When a more specific OSPF network range is removed, interfaces belonging to that network range are retained and remain active if, and only if, a less specific network range exists.

For example, consider the following configuration:

```
router ospf
   network 205.188.129.16 0.0.0.3 area 20
   network 205.188.129.40 0.0.0.3 area 20
   network 205.188.129.44 0.0.0.3 area 20
   network 205.188.129.96 0.0.0.3 area 20
   network 205.188.129.96 0.0.127.255 area 20
```

Enter the following:

```
no network 205.188.129.40 0.0.0.3 area 20
```

Interfaces falling into the network range 205.188.129.40/0.0.0.3 still remains active because the superset, 205.188.128.0/0.0.127.255, exists for area 20. A more specific network statement causes interfaces belonging to that range to be removed from a different area only if a less specific network statement (superset) exists.

Consider a configuration such as the following:

```
router ospf 1
  network 205.188.128.0 0.0.127.255 area 20
```

If the following network statement is entered:

```
network 205.188.129.96 0.0.0.3 area 40
```

the interfaces belonging to range 205.188.129.96/0.0.0.3 are removed from area 20 and moved to area 40. Network statements with identical ranges but different area IDs are considered as area changes. For example, the following network statements cause interfaces belonging to network range 205.188.129.40/0.0.0.3 to move from area 20 to area 40:

```
network 205.188.129.40 0.0.0.3 area 20
network 205.188.129.40 0.0.0.3 area 40
```

Examples

The following example shows how to initialize OSPF routing process. Area 0 enables OSPF.

```
ServiceRouter(config)# router ospf
ServiceRouter(config-ospf)# network 192.168.78.0 0.0.0.255 area 0
ServiceRouter(config-ospf)#
```

Related Commands

Command	Description
router ospf	Enables the OSPF routing process.

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 CDS device (including the **no** form of each command) vary based on whether the device is configured as a CDSM, 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.

Command Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

Valid values for *command* are as follows:

aaa	Configures AAA[1].
access-lists	Configures access control list entries.
acquirer	Configures acquisition parameters.
asset	Configures the asset tag name string.
authentication	Configures the authentication.
bandwidth	Configures bandwidth controls.
banner	Defines a login banner.
bitrate	Configures the bit rate.
cdsm	Configures the CDSM settings.
clock	Configures the time-of-day clock.
cms	Configures the CMS[2].
device	Configures the device mode.
direct-server-return	Configures direct-server-return.
disk	Configures disk-related settings.
dns	Configures the SE DNS cache.
exec-timeout	Configures the EXEC timeout.
external-ip	Configures up to eight external (NAT) IP addresses.
ftp	Configures FTP caching-related parameters.
help	Configures the assistance for the command-line interface.

hostname	Configures the system's network name.
http	Configures HTTP-related parameters.
icap	Configures the ICAP feature for the HTTP protocol.
interface	Configures a Gigabit Ethernet interface.
ip	Configures IP parameters.
ip access-list	Configures IP access lists.
kernel	Enables access to the kernel debugger.
ldap	Configures LDAP[3] parameters.
logging	Configures the syslog[4].
network-filesystem	Configures the network file system server and client.
ntp	Configures the NTP[5].
offline-operation	Configures the offline service operation.
pace	Configures the Movie Streamer 7H90C0CHand WMT pacing bandwidth and bit rate.
port-channel	Configures port channel global options.
primary-interface	Configures a primary interface.
radius-server	Configures RADIUS server authentication.
rtsp	Configures RTSP[6]-related parameters.
rule	Configures the Rules Template.
snmp-server	Configures the SNMP server.
sshd	Configures the SSH[7] service.
tcp	Configures global TCP parameters.
telnet enable	Configures Telnet services.
transaction-logs	Configures the transaction logging.
username	Establishes username authentication.
wmt	Configures WMT[8] parameters.

1. AAA = authentication, authorization, and accounting
2. CMS = Centralized Management System
3. LDAP = Lightweight Directory Access Protocol
4. syslog = system logging
5. NTP = Network Time Protocol
6. RTSP = Real-time Streaming Protocol
7. SSH = Secure Shell
8. WMT = Windows Media Technologies7H90C0CH

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 a Gigabit Ethernet or port channel command in interface configuration mode or set its defaults, use the **no** command in interface configuration mode.

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

Syntax Description

GigabitEthernet	Selects a Gigabit Ethernet interface to configure.
slot/*port*	Slot and port number for the selected interface. The slot range is 0 to 2; the port range is 0 to 3. The slot number and port number are separated with a forward slash character (/).
PortChannel	Selects the EtherChannel of interfaces to be configured.
1	Sets the port channel interface number to 1.
2	Sets the port channel interface number to 2.
Standby	Sets the standby group for the interface.
group_num	Group number for the selected interface. The group number range is 1 to 4.

Command Defaults

None

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).

Command Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

Use this command to synchronize the SE, SR or CDSM 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.

Note When the time is configured through **ntp server** command, then the **ntpdate** command should not be used to set the time. If **ntpdate** is used then, an error message will be displayed.

When you synchronize the CDSM clock with an NTP server, there is a possibility of all devices registered with the CDSM being shown as offline and then reverted to online status. This situation can occur when synchronization with the NTP server sets the CDSM clock forward in time by an interval greater than at least two polling intervals or when the software clock on the CDSM is changed by a similar value using the **clock** command in EXEC configuration mode. The CDSM determines the status of devices in the CDS network depending on when it was last contacted by the devices for a getUpdate request. If you set the CDSM clock ahead in time, you have added that amount of time to the period since the CDSM received the last getUpdate request. However, it is only a transient effect. Once the devices contact the CDSM for their next getUpdate request after the clock setting change, the CDSM 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 172.16.22.44
```

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

```
ServiceEngine(config)# no ntp 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 status	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.

Command 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.

On the CDSM and SE:

ping {*hostname* | *ip_address*}

On the SR:

ping {*hostname* | *ip_address* | **srp** {*hostname* | *ip_address*}}

Syntax Description

hostname	Hostname of system to ping.
ip_address	IP address of system to ping.
srp	Pings the Service Routing Protocol.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

To use this command with the *hostname* argument, be sure that 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#
```

ping srp

To ping the Service Routing Protocol ring, use the **ping** command in EXEC configuration mode.

ping srp

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

In an ipv4 or ipv6 environment, the **ping** command uses the ipv4 or ipv6 address. The **ping srp** command uses The DHT key (64 bits hex-id).

In the example below, the node that owns the DHT key (node SR-205-5) responds to this ping. The TTL is 64, and the response time is 0.330585 ms.

Examples

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

```
ServiceRouter# ping srp
6aab6568d794a77bc20633b0cb3aef14d906e4aef00a3fa2a93973524337e40c
Ping response from SR-205-5:9000, ttl=64, time=0.330585 ms
  id=6aab6568d794a77bc20633b0cb3aef14d906e4aef00a3fa2a93973524337e40c
Ping response from SR-205-5:9000, ttl=64, time=0.282069 ms
  id=6aab6568d794a77bc20633b0cb3aef14d906e4aef00a3fa2a93973524337e40c
Ping response from SR-205-5:9000, ttl=64, time=0.278821 ms
  id=6aab6568d794a77bc20633b0cb3aef14d906e4aef00a3fa2a93973524337e40c
Ping response from SR-205-5:9000, ttl=64, time=0.279144 ms
  id=6aab6568d794a77bc20633b0cb3aef14d906e4aef00a3fa2a93973524337e40c
Ping response from SR-205-5:9000, ttl=64, time=0.283236 ms
  id=6aab6568d794a77bc20633b0cb3aef14d906e4aef00a3fa2a93973524337e40c

ServiceRouter#
```

Related Commands

Command	Description
traceroute srp	Traces the route of the Service Routing Protocol ring.

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.

Command 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-port** | **round-robin** | **src-dst-mac** | **src-dst-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 MAC addresses.
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-port	Specifies the load balancing method using source and destination port.
src-port	Specifies the load balancing method using source Layer 4 port.

Command 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 Internet Streamer CDS 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 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 CDS is determined by the switch, this applies to all application traffic over port channels.

Note 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 CDS 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 CDS 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 CDS network primary interface.
1-2	Port channel number 1 or 2.
Standby	Selects a standby group as the CDS network primary interface.
group_num	Standby group number.

Command 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 CDSM, the CDSM uses the configured primary interface to communicated with the registered devices.

You cannot enable the CDS 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 CDS 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 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 CDS network.

The primary interface can be changed without disabling the CDS 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 CDS network, if you want to re-enable the CDS 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
```

proximity algorithm bgp

To enable a Border Gateway Protocol (BGP) proximity algorithm option for the Proximity Engine, use the **proximity algorithm bgp** command in Global configuration mode. To disable a BGP proximity algorithm option, use the **no** form of the command.

proximity algorithm bgp {**best-path** | **location-community** [**strict**] | **redirect**}

no proximity algorithm bgp {**best-path** | **location-community** [**strict**] | **redirect**}

Syntax Description

best-path	Specifies the BGP Autonomous Systems (AS) path length-based proximity.
location-community	Specifies that the community-based proximity algorithm be used.
strict	(Optional) Strict matching.
redirect	Specifies the BGP AS-based redirection.

Command Defaults

By default, the BGP algorithms are turned off.

Command Modes

Global configuration (config) mode.

Usage Guidelines

When BGP is configured as the routing protocol, the **proximity algorithm bgp** command enables a BGP proximity option for the Proximity Engine. The **Proximity algorithm bgp** commands are not effective unless BGP is configured first.

Best-Path

When the BGP routing protocol is configured the Proximity Engine learns routes from other AS, and therefore can rank proximity target addressees (PTAs) that originate in an external AS using not only the basic BGP proximity (which ranks the PTAs based on their next-hop), but also based on the AS path length of the PTAs. This capability is enabled by the **proximity algorithm bgp best-path** command. A PTA that has a longer AS path length is less preferred. It should be noted that the Proximity Engines takes into account the AS path length of the PTAs only if the proximity source address (PSA) is originated in the same AS as the Proximity Engine, since the AS path length learnt by the Proximity Engine is with reference to its own AS. If the PSA originates in an external AS, it is recommended that the **proximity algorithm bgp redirect** be enabled to redirect the request to a Proximity Engine in the same AS as the PSA if such a Proximity Engine exists.

Location Community

When the **proximity algorithm bgp location-community** command is enabled, additional location information is included in the proximity calculation to influence application-level traffic optimization in the network. Many service providers are already using BGP community values to identify prefixes originated from a given POP. Taking advantage of the community information can greatly improve the scalability and flexibility of the proximity calculation algorithm.

BGP community-based proximity is used when community-based proximity option is enabled and the PSA has a BGP community string that is configured in the **location community** command. PTAs that have the same BGP community string as the PSA are ranked as more preferred than PTAs that do not have the same BGP community string as the PSA. For the remaining PTAs that have different community strings, they are ranked by either IGP or BGP proximity.

Community-based proximity requires the use of the **location community** command to configure the Proximity Engine community values. Each Proximity Engine must be configured with the community numbers that are used within the network to locate the prefix origination point.

When community values are configured, the Proximity Engine creates and maintains a sorted table of communities within BGP. Currently, location community configurations must be manually configured on each Proximity Engine.

Redirect

If the PSA, where the proximity request is initiated, is learned from another AS, the current Proximity Engine does not have the best knowledge to handle the proximity request. If the proximity redirect option is enabled, the Proximity Engine sends back a Redirect response to the Service Router. The Redirect response contains the list of Proximity Engines that reside in the same AS as the PSA. The Service Router then sends the proximity request to one of these Proximity Engines.

Configuring Proximity Algorithm BGP

Perform the following steps to configure Proximity Algorithm BGP:

Step 1 Turn on BGP Best Path algorithm in the Proximity Engine.

```
ServiceRouter(config)# proximity engine enable
ServiceRouter(config)# proximity algorithm bgp best-path
```

Step 2 Enable router bgp 1:

```
ServiceRouter(config)# router bgp 1
ServiceRouter(config)# neighbor 26.0.0.6 remote-as 1
```

Step 3 Turn on EBGP in the routers.

Result Analysis

When PSA is 3.1.5.0 and PTA is 33.1.5.0, the returned proximity cost is 2164260884.

```
ServiceRouter# show ip rib route

3.1.5.0/24, 1 ucast next-hops, 0 mcast next-hops, attached
*via 3.1.5.3, GigabitEthernet 1/0, [0/0], 00:01:59, direct
26.0.0.0/8, 1 ucast next-hops, 0 mcast next-hops, attached
*via 26.0.0.2, GigabitEthernet 2/0, [0/0], 00:01:59, direct
33.1.5.0/24, 1 ucast next-hops, 0 mcast next-hops
*via 26.0.0.6, GigabitEthernet 2/0, [200/0], 00:00:29, bgp-1, internal, tag 2
extended route information: AS Hops 1, BGP PxEer AS 1
62.0.0.0/8, 1 ucast next-hops, 0 mcast next-hops
*via 26.0.0.6, GigabitEthernet 2/0, [115/20], 00:01:27, isis-p1, L1
```

The AS Path length can be calculated from the **show ip route** command:

AS Path length for PTA 33.1.5.0 - 1

The 31st community bit set to 1 since no location community match, AS Path length is 1(set the 24th bit to 1), the IGP cost is 20.

2147483648+ 16777216 + 20 = 2164260884

The proximity calculation rendered using the following formula:

rating(PSA,PTA)= 2^31Cc comm_match(PSA,PTA) +2^24CBPAS_path_len(PTA)+ IGP_rating(PSA,PTA)

- The result is given in 32 bits.
- The 31st Location community is zero if the location community matches. It is effective only when the BGP location community algorithm is turned on.
- The bits (24-30) denote the AS Best path distance. It is effective only on turning on the BGP redirect algorithm.
- The the remaining 24 bits hold the IGP rating returned by the IGP daemons. The IGP daemons returns 32-bit values that are normalized to occupy the 24 bits.

Examples

Proximity Algorithm Redirect

The following example shows how to use the proximity redirect option:

```
ServiceRouter(config)# proximity algorithm bgp redirect
```

First, each Proximity Engine must form a DHT ring.

```
ProximityEngine1(config)# router srp
ProximityEngine1(config-srp)# domain 100

ProximityEngine2(config)# router srp
ProximityEngine2(config-srp)# domain 100
ProximityEngine1(config-srp)# bootstrap 3.4.0.7
```

Configure both the Proximity Servers on the Service Router and enable proximity-based-routing:

```
ServiceRouter(config)# service-router proximity-based-routing proximity-server 3.4.0.7
ServiceRouter(config)# service-router proximity-based-routing proximity-server 3.1.14.17
ServiceRouter(config)# service-router proximity-based-routing enable
```

Next, enable BGP on both the Proximity Engines such that both are in different AS:

```
ProximityEngine1(config)# router bgp 1
ProximityEngine1(config-bgp)# neighbor 3.4.0.12 remote-as 1

ProximityEngine2(config)# router bgp 2
ProximityEngine2(config-bgp)# neighbor 3.1.14.12 remote-as 2
```

For Proximity Redirect to work efficiently, it is recommended that there are at least two Proximity Servers, one each in a different autonomous system.

In the above example each Proximity Engine is connected with routers and routers advertise the routes to the respective Proximity Engines and the neighbor IP addresses are the corresponding neighbor router's directly connected interfaces:

```
ProximityEngine1# sh ip bgp all

BGP routing table information for address family IPv4 Unicast
BGP table version is 5, local router ID is 3.4.0.7
Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid, >-best
Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist
Origin codes: I - IGP, E - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Path
```

```
*>i3.1.14.0/24 3.4.0.12 0 100 0 2 I
*>i3.4.0.0/16 3.4.0.12 0 100 0 I

BGP routing table information for address family IPv4 Multicast

ProximityEngine2# sh ip bgp all

BGP routing table information for address family IPv4 Unicast
BGP table version is 5, local router ID is 3.4.0.8
Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid, >-best
Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist
Origin codes: I - IGP, E - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Path
*>i3.1.14.0/24 3.1.14.12 0 100 0 I
*>i3.4.0.0/16 3.1.14.12 0 100 0 1 I

BGP routing table information for address family IPv4 Multicast
```

Next, it needs to be checked if the DHT Ring is formed appropriately:

```
ServiceRouter# show srp neighbor
Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
I - Intransitive, R - Replicate Set, D - delay, ND - New Delay
H - hold time, U - up time

Number of neighbors in the database: 1
RPL c152b683f000c6be3ff82214e4d8084d52a44dee85b29d67c49e60fbaf3e4737
via U6-CDE205-2 [3.1.14.17] 9000, D=0.223891 ms, ND=0.230440 ms
H=00:00:07, U=00:00:15

ProximityEngine2# show srp neighbor

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
I - Intransitive, R - Replicate Set, D - delay, ND - New Delay
H - hold time, U - up time

Number of neighbors in the database: 1
RPL 97d35b9f3cb020799d9cbfec2adcca50e9644f2613f041648734459d29f88a0d
via U6-CDE205-1 [3.4.0.7] 9000, D=0.229732 ms, ND=0.223568 ms
H=00:00:08, U=00:00:22
```

Where 3.4.0.7 is ProximityEngine1's interface and 3.1.14.17 is ProximityEngine2's interface and is stored in each other tables.

When a request arrives from the client machine, whose client IP belongs to the 3.4.0.0/16 network (which happens to be from AS-1), say for example, 3.4.0.10, the SR looks up in the configured Proximity Servers and selects the Proximity Server with the lowest IP address, which in this case happens to be 3.1.14.17.

The SR would send the SOAP request with the PSA 3.4.0.10 to ProximityEngine2 (3.1.14.17).

ProximityEngine2, would lookup the URIB table to find out if there is another Proximity Engine from the same AS. Since, in this case, there is ProximityEngine1 in AS-1 from where the request has emanated, it returns a Redirect message with ProximityEngine1's IP address as the request end-point.

The SR redirects the SOAP request to the ProximityEngine1.

ProximityEngine1 would look up its URIB table and return the cost for the available PTAs.

The Service Router, upon receiving the cost from the ProximityEngine1, would choose the PTA with lowest cost and give the SE redirection to the client.

The client would now contact the SE and play the content.

Community-Based Proximity Algorithm Example

The following example shows how to use the **proximity algorithm bgp** command to enable the community-based proximity algorithm:

```
ServiceRouter(config)# proximity algorithm bgp location-community
ServiceRouter(config)# exit
ServiceRouter# show ip proximity algorithm
Proximity algorithm: bgp community
```

The following example shows how to configure community values. In this example, the first **location community** command configures the community value 100:10 and the second command configures community values from 100:100 to 100:200:

```
ServiceRouter(config)# router bgp 23
ServiceRouter(config-bgp)# location community 100:10
ServiceRouter(config-bgp)# location community 100:100-100:200
```

The following example shows how to enable the proximity redirect option:

```
ServiceRouter(config)# proximity algorithm bgp redirect
```

First, each Proximity Engine must form a DHT ring:

```
ServiceRouter(config)# router srp
ServiceRouter(config-srp)# domain 100
ServiceRouter(config-srp)# bootstrap 192.168.10.1
```

Each Proximity Engine must advertise its interface address to the BGP cloud by configuring IGP for OSPF and IS-IS or configuring BGP with the neighbor.

The following example is for OSPF:

```
ServiceRouter(config)# router ospf
ServiceRouter(config-ospf)# network 192.168.10.0 255.255.255.0 area 0
```

The following example is for configuring BGP:

```
ServiceRouter(config)# router bgp
ServiceRouter(config-bgp)# neighbor 192.168.82.1 remote-as 23
```

The following examples shows how to configure the BGP AS path length-based proximity. This example is for the same AS configuration:

```
ServiceRouter(config)# proximity algorithm bgp best-path
ServiceRouter(config)# router bgp 23
ServiceRouter(config-bgp)# neighbor 192.168.82.1 remote-as 23
```

The following example is for a different AS configuration:

```
ServiceRouter(config)# proximity algorithm bgp best-path
ServiceRouter(config)# router bgp 10
ServiceRouter(config-bgp)# neighbor 192.168.82.1 remote-as 23
```

Proximity Algorith BGP Best-Path Example

The following example shows how to turn on the BGP Best-Path algorithm:

```
ProximityEngine(config)# proximity algorithm bgp best-path

ProximityEngine# show ip bgp 3.1.14.0
BGP routing table entry for 3.1.14.0/24, 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
3.4.0.12 (metric 0) from 3.4.0.12 (3.4.0.12)
Origin IGP, MED 0, localpref 100, weight 0
Community: 1:1

Not advertised to any peer
```

The following is a sample of the service-router logs with respect to the cost returned by the Proximity Engine:

```
02/08/2010 07:34:42.290(Local)(5792)TRCE:SRNetProxClient.cpp:86->
Target
Hostname => U6-WAE612-2
IpAddress => 3.4.0.14
Rating => 2147483648
02/08/2010 07:34:42.290(Local)(5792)TRCE:SRNetProxClient.cpp:86->
Target
Hostname => U6-WAE612-1
IpAddress => 3.1.14.7
Rating => 2164260864
```

In the previous example, since the PTA 3.1.14.7 has a higher cost, the PTA 3.4.0.17 gets a higher preference owing to the lower cost.

The following example shows how to verify proper connectivity between the two Proximity Engines:

```
ProximityEngine1# show srp neighbor
Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
I - Intransitive, R - Replicate Set, D - delay, ND - New Delay
H - hold time, U - up time

Number of neighbors in the database: 1
RPL c152b683f000c6be3ff82214e4d8084d52a44dee85b29d67c49e60fbaf3e4737
via U6-CDE205-2 [3.1.14.17] 9000, D=0.395056 ms, ND=0.378471 ms
H=00:00:09, U=00:38:37

ProximityEngine1# show srp database
c9bc3e170457a6a08d8a218a15a00d8feb73e4295d06f7e014b6f66fee01c9e4: 793
```

Enter the same commands to check the SRP connection on the other Proximity engine:

```
ServiceRouter# show srp neighbor
Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
I - Intransitive, R - Replicate Set, D - delay, ND - New Delay
H - hold time, U - up time

Number of neighbors in the database: 1
RPL 97d35b9f3cb020799d9cbfec2adcca50e9644f2613f041648734459d29f88a0d
via U6-CDE205-1 [3.4.0.7] 9000, D=0.495889 ms, ND=0.470399 ms
H=00:00:07, U=00:40:57

ProximityEngine2# show srp database
c9bc3e170457a6a08d8a218a15a00d8feb73e4295d06f7e014b6f66fee01c9e4: 793
```

Related Commands

Command	Description
show ip proximity algorithm	Displays the proximity algorithm options currently in use by this Proximity Engine.

proximity engine enable

To enable the Proximity Engine, use the **proximity engine enable** command in Global configuration mode. To disable the Proximity Engine, use the **no** form of this command.

proximity engine enable

no proximity engine enable

Syntax Description

This command has no arguments or keywords.

Command Modes

Global configuration (config) mode.

Usage Guidelines

The Proximity Engine is a device mode which needs to be enabled on the Service Router in order to enable dynamic routing protocols OSPF/IS-IS/BGP. You can turn on the Proximity Engine functionality using the **proximity engine enable** command. Only after enabling the Proximity Engine, all the routing functionality is enabled and related commands are unlocked. Once the Proximity Engine is enabled, you can turn on either OSPF or IS-IS for IGP and/or BGP. But in the Proximity Engine device, we do not make use of the OSPF process-id, which we generally do on the router.

When disabling the Proximity Engine after issuing the **no proximity engine enable** command, you are asked to confirm this action because all Proximity Engine configurations are lost when you enter this command.

Examples

The following example shows how to enable the Proximity Engine:

```
ServiceRouter# configure terminal
ServiceRouter(config)# proximity engine enable
```

The following example shows how to disable the Proximity Engine:

```
ServiceRouter# configure terminal
ServiceRouter(config)# no proximity engine enable
All Proximity Engine configuration will be lost! Proceed? [ no ] yes
ServiceRouter(config)#
```

The following example shows how to enable OSPF:

```
ServiceRouter# config
ServiceRouter (config)# proximity engine enable
Starting Proximity Engine ....
Proximity Engine Started.
ServiceRouter (config)# router ospf
ServiceRouter (config-ospf)# network 15.0.0.0 ?
  A.B.C.D  IP wildcard mask
ServiceRouter (config-ospf)# network 15.0.0.0 0.255.255.255 ?
  area  Configure area properties
ServiceRouter (config-ospf)# network 15.0.0.0 0.255.255.255 area 0 ServiceRouter#
ServiceRouter (config-ospf)#
```

Note OSPF process ID is used.

Enter the following commands on the router:

```
Router (config)# router ospf 1
Router (config-ospf)# network 15.0.0.0 0.255.255.255 area 0
Router (config-ospf)#

<Turned on OSPF debugging on Router>

*Jun 29 01:14:08.642: OSPF: Interface GigabitEthernet0/0 going Up *Jun 29 01:14:09.142:
OSPF: Build router LSA for area 0, router ID 2.2.2.2, seq 0x80000001, process 1 *Jun 29
... Output omitted

<2.2.2.2 is the Router-id of the Router>
```

Verify adjacency on the Proximity Engine by entering the following commands:

```
ServiceRouter# show ip ospf route
 OSPF Process ID p1 context default, Routing Table
  (D) denotes route is directly attached      (R) denotes route is in
RIB
15.0.0.0/8 (intra)(D) area 0
     via 15.0.0.1/GigabitEthernet 2/0*, cost 65535, adv router 3.1.5.2

ServiceRouter# show ip ospf database
        OSPF Router with ID (3.1.5.2) (Process ID p1 context default)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link
Count
2.2.2.2         2.2.2.2         140         0x80000002 0xb04d   1
3.1.5.2         3.1.5.2         140         0x80000002 0x100d   1

                Network Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
15.0.0.1        3.1.5.2         140         0x80000001 0x2408
```

The following example shows how to enable BGP:

```
ServiceRouter# config
ServiceRouter(config)# proximity algorithm bgp location-community
!
ServiceRouter(config)# router bgp 1
ServiceRouter(config-bgp)# neighbor 5.45.1.101 remote-as 1 <-- configures a BGP peer in
Autonomous System (AS) 1. This peer advertises BGP routes to the PxE.
ServiceRouter(config-bgp)# location community 1:1 <-- configures 1:1 as a
location-community used by BGP location-community proximity algorithm.
ServiceRouter(config-bgp)# exit
```

The following example shows how to enable IS-IS:

```
ServiceRouter# config
ServiceRouter(config)# router isis
ServiceRouter(config-isis)# net 49.0000.0000.0205.0002.00 <-- Configures the Network
Entity Title (NET).
ServiceRouter(config-isis)# interface GigabitEthernet 1/0 <-- PxE interface actively
running IS-IS.
ServiceRouter(config-isis)# ip router isis
ServiceRouter(config-isis)# exit
ServiceRouter(config-isis)# interface GigabitEthernet 2/0 <-- PxE interface actively
running IS-IS.
```

```
ServiceRouter(config-isis)# ip router isis
ServiceRouter(config-isis)# exit
```

The following example shows how to enable SRP:

```
ServiceRouter# config
ServiceRouter(config)# router srp
ServiceRouter(config-srp)# bootstrap 172.20.168.89 <-- A boot-strap-node is an existing
member of the DHT ring.
ServiceRouter(config-srp)# domain 1 <-- All SRP nodes have the same domain number to be in
a DHT ring
ServiceRouter(config-srp)# exit
```

Related Commands

Command	Description
service-router proximity-based-routing	Configures proximity-based routing on the Service Router.

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.

Command 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, 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).

Command 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 an CDS network device to authenticate users attempting to connect to a network device. The CDS network device functions as a client, passing user information to one or more RADIUS servers. The CDS 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 2-292.
- 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 2-293.

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 CDSM GUI or the CLI to enable RADIUS authentication on an SE.

Tip From the CDSM 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 RTSP traffic.
show radius-server	Displays RADIUS information.

rcp

To enable the Remote Copy Program (RCP), use the **rcp** command in Global configuration mode. To disable RCP, use the **no** form of this command.

rcp enable

no rcp enable

Syntax Description

enable	Enables RCP services.

Command Defaults

None

Command Modes

Global configuration (config) mode.

Examples

The following example shows how to enable RCP:

```
ServiceEngine(config)#  rcp enable
```

Related Commands

Command	Description
show rcp	Displays RCP 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.

Command 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 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.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use this command to rename any 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.

Command 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 CDSM database and copy the backup file to a safe location that is separate from that of the CDSM, or change over from the primary to a standby CDSM before you use the **restore factory-default** command on your primary CDSM. The primary CDSM 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 CDSM 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 CDSM database, all configuration records for the entire CDS network are deleted. If you do not have a valid backup file or a standby CDSM, you must use the **cms deregister force** command and reregister every SE and SR after you have reconfigured the CDSM, because all previously configured data is lost.

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

If you created a backup file while you configured the primary CDSM, you can copy the backup file to this newly reconfigured CDSM 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.

Cisco Internet Streamer CDS 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 Cisco Internet Streamer CDS 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 CDS network after using the **restore factory-default preserve basic-config** command, reconfigure the primary interface after the factory defaults have been restored.

```
CDSM# restore factory-default
This command will wipe out all of data on the disks
and wipe out CDS 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 ]

CDSM# restore factory-default preserve basic-config
This command will wipe out all of data on the disks
and all of CDS 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.

The **show wmt** command continues to display the same license evaluation periods as before the **restore factory-default** command was invoked, because the evaluation period is not affected by this **restore** command. For example, if there were 21 days remaining in the evaluation period before the **restore factory-default** command was used, there would continue to be 21 days remaining in the evaluation period.

Related Commands

Command	Description
cms database backup	Backs up the existing management database for the CDSM.
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.
show wmt	Displays WMT bandwidth and proxy mode 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.

Command 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, 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.

router bgp

To configure a BGP routing process, use the **router bgp** command in Global configuration mode. To remove a BGP routing process, use the **no** form of this command.

router bgp *as_number*

no router bgp *as_number*

Syntax Description

as_number	Number of an Autonomous System (AS) that identifies the router to other BGP routers, and tags the routing information that is passed along.

Command Defaults

No BGP routing process is configured.

Command Modes

Global configuration (config) mode.

Usage Guidelines

This command is used to set up a distributed routing core that automatically guarantees the loop-free exchange of routing information between autonomous systems.

Enable the Proximity Engine by entering the **proximity engine enable** command before executing this command.

For the proximity function to work, one of the following is required:

- Enabled link-state protocol, such as OSPF or IS-IS for IGP proximity.
- Enabled policy routing protocol, such as BGP for best-path proximity, and one of the IGP (OSPF or IS-IS) is required for next hop resolution.

Note All BGP routes must resolve to IGP next hops or directly connected routes.

Examples

The following example shows how to configure a BGP process for autonomous system 23:

```
ServiceRouter(config)# router bgp 23
ServiceRouter(config-bgp)#
```

Related Commands

Command	Description
location community	Configures the community values that are associated with a Proximity Engine.
log-neighbor-changes	Enables logging of BGP neighbor resets.
neighbor	Configures the BGP neighbors.

router isis

To enable the IS-IS routing protocol and to specify an IS-IS process, use the **router isis** command in Global configuration mode. To disable IS-IS routing, use the **no** form of this command.

router isis

no router isis

Syntax Description

This command has no arguments or keywords.

Command Defaults

IS-IS routing is disabled.

Command Modes

Global configuration (config) mode.

Usage Guidelines

This command is used to enable routing for an area. An appropriate network entity title (NET) must be configured to specify the area address and the system ID of the router. Routing must be enabled on one or more interfaces before adjacencies can be established and dynamic routing is made possible.

Enable the Proximity Engine by entering the **proximity engine enable** command before executing this command.

Note It is not possible to configure IS-IS and OSPF simultaneously. If you are running OSPF and try to enter the **router isis** command, you receive the following warning message:

```
%Cannot configure both IS-IS and OSPF together. Please remove 'router ospf' first. (Error
number: 1137)
```

If you want to configure IS-IS and you already have OSPF running, you must enter the **no router ospf** command first before entering the **router isis** command.

Examples

The following example shows how to configure IS-IS for IP routing. In this example, system ID is set to 0001.0c11.1111.00 and area is set to ID 47.0004.004d.0001. IS-IS is configured to form adjacencies on Ethernet interface 0 and serial interface 0. The IP prefix assigned to Ethernet interface 0 is advertised to other IS-IS routers.

```
ServiceRouter# show node-type
PROXIMITY_ENGINE

ServiceRouter# config t
ServiceRouter(config)# router isis
ServiceRouter(config-isis)# net 47.0004.004d.0001.0001.0c11.1111.00
ServiceRouter(config-isis)# interface GigabitEthernet 1/0
ServiceRouter(config-isis-if)# ip router isis
ServiceRouter(config-isis-if)# end
ServiceRouter#
```

Related Commands

Command	Description
authentication	Configures the authentication parameters.
authentication-check	Enables the checking of received packets on the corresponding level.
authentication-type	Specifies the cleartext or MD5 authentication for the corresponding level.
interface	Configures a Gigabit Ethernet or port channel interface. Provides access to interface configuration mode.
is-type	Configures a Proximity Engine to act as a Level 1 (intra-area) router, as both a Level 1 router and a Level 2 (intra-area) router, or as an inter-area router only.
log-adjacency-changes	Configures the router to send a syslog message when an IS-IS neighbor goes up or down.
lsp-mtu	Sets the maximum transmission unit MTU size of IS-IS LSPs.
net	Configures an IS-IS NET for a CLNS routing process.

router ospf

To enable the Open Shortest Path First (OSPF) routing process, use the **router ospf** command in Global configuration mode. To terminate the OSPF process, use the **no** form of this command.

router ospf

no router ospf

Syntax Description

This command has no arguments or keywords.

Command Defaults

This command is disabled by default.

Command Modes

Global configuration (config) mode.

Usage Guidelines

For Proximity Engine, the fixed process ID "p1" is used internally. This allows only one instance of the OSPF process, but it supports multiple areas. Routing must be enabled on one or more interfaces before adjacencies can be established and before dynamic routing is possible.

Enable the Proximity Engine by entering the **proximity engine enable** command before executing this command.

Note It is not possible to configure IS-IS and OSPF simultaneously. If you are running IS-IS and try to enter the **router ospf** command, you receive the following warning message:

%Cannot configure both IS-IS and OSPF together. Please remove 'router ospf' first. (Error number: 1137)

If you want to configure OSPF and you already have IS-IS running, you must enter the **no router isis** command first before entering the **router ospf** command.

Examples

The following example shows how to configure an OSPF routing process:

```
ServiceRouter# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ServiceRouter(config)# router ospf
ServiceRouter(config-ospf)# end
ServiceRouter#
```

Related Commands

Command	Description
area	Configures the area.
authentication	Configures the authentication parameters.
authentication-check	Enables the checking of received packets on the corresponding level.
authentication-type	Specifies the cleartext or MD5 authentication for the corresponding level.
interface	Configures a Gigabit Ethernet or port channel interface. Provides access to interface configuration mode.
log-adjacency-changes	Configures the router to send a syslog message when an IS-IS neighbor goes up or down.
network area	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.

router srp

To enter SRP configuration mode, use the **router srp** command in Global configuration mode. To negate the SRP daemon and remove all SRP running configuration, use the **no** form of this command.

router srp

no router srp

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

This command is used to enter SRP configuration mode, where a system administrator can configure different parameters of the SRP.

Enable the Proximity Engine by entering the **proximity engine enable** command before executing this command.

For SRP to run properly, it is necessary to configure the NTP server on the SR. Configure NTP as follows:

```
ServiceRouter(config)# ntp server 171.68.10.150
ServiceRouter(config)# end
ServiceRouter# sh ntp status ntp enabled server list: 2.8.1.2 171.68.10.150
remote refid st t when poll reach delay offset jitter
==============================================================================
2.8.1.2 0.0.0.0 16 u - 64 0 0.000 0.000 4000.00
*ntp-sj1.cisco.c ntp02-syd.cisco 2 u 63m 137m 177 1.625 -1.806 0.881
ServiceRouter#
```

Examples

The following example shows the use of **router srp**:

```
ServiceRouter# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ServiceRouter(config)# router srp
ServiceRouter(config-srp)#
```

Related Commands

Command	Description
bootstrap-node	Configures a bootstrap node IP address.
domain	Sets the domain ID for an SRP.
flooding	Configures the flooding threshold.

rtsp

To configure the Real-Time Streaming Protocol (RTSP)-related parameters, use the **rtsp** command in Global configuration mode. To disable individual options, use the **no** form of this command.

rtsp {**advanced** *ip_address* {**bypass-gateway movie-streamer | max-initial-setup-delay** *time_delay* **| max-request-rate** *num*} **| ip-address** *ip_address*}

no rtsp {**advanced** *ip_address* {**bypass-gateway movie-streamer | max-initial-setup-delay** *time_delay* **| max-request-rate** *num*} **| ip-address** *ip_address*}

Syntax Description

advanced	Performs advanced configuration of the RTSP gateway.
ip_address	The IP address of RTSP gateway.
bypass-gateway	Allows bypassing the RTSP gateway for RTSP requests.
movie-streamer	Allows bypassing the RTSP gateway for Movie Streamer RTSP requests.
max-initial-setup-delay	Specifies the maximum delay, in seconds, between the TCP accept and first RTSP message from the client. The default is 10.
time_delay	The RTSP advanced maximum initial setup delay, in seconds. The range is from 0 to 2147483647.
max-request-rate	Specifies the maximum incoming requests allowed by the RTSP Gateway per second.
num	The maximum requests per second. The range is from 1 to 2147483647.
ip-address	Configures the IP address for the RTSP gateway.

Command Defaults

max-initial-setup-delay *time_delay*: 10

max-request-rate *num*: 40 requests

Command Modes

Global configuration (config) mode.

Usage Guidelines

Real-Time Streaming Protocol (RTSP) is a standard Internet streaming control protocol (RFC 2326). It is an application-level protocol that controls the delivery of data with real-time properties, such as video and audio. Apple QuickTime, Real Networks, and the Cisco Streaming Engine use RTSP as the streaming control protocol.

Live Streaming with the Cisco Streaming Engine

The Internet Streamer CDS software supports live streaming content with many kinds of network topologies and deployment scenarios. This feature allows the integration of streaming content from Cisco IP/TV Servers and QuickTime live broadcast servers with the CDS network. Support for broadcast of playlists is included (except for SEs at the network edge), allowing you to convert one or more disk files into a playlist and to send them out through simulated live streaming.

An RTSP source is a fully qualified RTSP URL that references an external streaming server, such as a parent SE, which provides the corresponding RTSP request point.

RTSP Gateway

The RTSP gateway is a process that runs on the SE. The RTSP gateway accepts an RTSP request and performs the initial RTSP handshake with RTSP-based clients (for example, Windows Media 9 players) on behalf of the back-end RTSP servers (for example, the WMT RTSP server) that are running on the SE.

For every RTSP request, the RTSP gateway examines the following properties of the request:

- URL and its position in the Unified Name Space (UNS)
- User agent
- IP address of the final destination
- Media type

After the successful completion of uniformity checks, the RTSP gateway tunnels the request to the appropriate back-end RTSP server that is running on the SE. The RTSP gateway can tunnel the request to RealProxy, RealSubscriber, or the Cisco Streaming Engine on the SE, depending on the requested media type, the back-end RTSP servers that are currently enabled on the SE, and the media player that is requesting the content.

After the RTSP gateway tunnels the request to a particular back-end RTSP server that is running on the SE and the back-end server and the client negotiate the UDP ports, the RTSP gateway continues with RTSP message passing (SETUP). When the RTSP client issues a PLAY request, the streaming server starts streaming the data to the client over UDP.

Based on the properties of the incoming request, including user agent, final destination, and media file type, the RTSP gateway performs the following tasks with SEs:

- Forwards the incoming request to the appropriate back-end RTSP server that is running on the SE. The incoming request goes to the WMT RTSP server if the client is a Windows Media 9 player. The SE uses the IETF standard RTSP protocol and proprietary Microsoft extensions to serve the content to Windows Media 9 players.
- Redirects the incoming request.
- Rejects the incoming request.

If the SE is registered with a CDSM, the RTSP gateway also redirects the incoming requests to other content distributors (for example, RealSubscriber or Cisco Streaming Engine) that are configured on the SE.

Network Address Translation (NAT) is designed for IP address simplification and conservation because it enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT operates on a router, usually connecting two networks together, and translates the private addresses in the internal network into legal addresses before packets are forwarded onto another network. As part of this functionality, NAT can be configured to advertise only one external address for the entire network. This configuration provides additional security, effectively hiding the entire internal network from the world behind that address. NAT has the dual functionality of security and address conservation and is typically implemented in remote access environments.

Note If the SE is behind a NAT-enabled router, you must specify the IP address of the RTSP gateway that is running on the SE. By default, no IP address is specified.

Default RTSP Gateway Settings

The RTSP gateway is automatically enabled on the SE and cannot be disabled with a command. Table 2-11 lists the default settings for the RTSP gateway.

Table 2-11 Default Settings for the RTSP Gateway

RTSP Gateway Setting	Default Setting
IP address of RTSP gateway	Not specified
Incoming RTSP port	Port 554
Incoming RTSP request rate	40 requests per second
Layer 4 switching	Not enabled
Maximum initial setup delay	10 seconds
Maximum request rate	40 requests per second

By default, the RTSP gateway is always enabled on an SE and cannot be disabled by entering a CLI command. As Table 2-11 shows, the RTSP gateway has a set of default settings. You only need to change these default settings under the following conditions:

- You want to configure the RTSP gateway to listen for incoming RTSP requests on a port other than the default port (port 554).
- SE is behind a NAT-enabled router. In this case, you must specify the IP address of the RTSP gateway. By default, an IP address for the RTSP gateway is not specified.

Note A description of the RTSP is available as IETF RFC 2326.

Examples

The following example shows how to set up the Movie Streamer RTSP bypass gateway:

```
ServiceEngine(config)# rtsp advanced bypass-gateway movie-streamer
```

The following example shows how to establish the maximum initial setup delay:

```
ServiceEngine(config)# rtsp advanced max-initial-setup-delay 15
```

The following example shows how to establish the maximum request rate:

```
ServiceEngine(config)# rtsp advanced max-request-rate 50
```

The following example shows how to assign the RTSP IP address:

```
ServiceEngine(config)# rtsp ip-address 10.74.61.1
```

Related Commands

Command	Description
show rtsp	Displays the RTSP configurations.

rule

To set the rules by which the SE filters HTTP, HTTPS, and RTSP traffic, use the **rule** command in Global configuration mode. To disable individual options, use the **no** form of this command.

rule action {**allow pattern-list** *list_num* [**protocol** {**all** | **http** | **https** | **rtsp**}] | **block pattern-list** *list_num* [**protocol** {**all** | **http** | **https** | **rtsp**}] | **generate-url-signature** {**include-client-src-ip** | **key-id-owner** *key_id* {**key-id-number** *key_id_number*} {**pattern-list** *patterm_list_num*} [**protocol** {**all** | **http**}]} | **no-cache pattern-list** *list_num* [**protocol**{**all** | **http** | **https**}] | **redirect** *url* **pattern-list** *list_num* [**protocol** {**all** | **http** | **https** | **rtsp**}] | **refresh pattern-list** *list_num* [**protocol** {**all** | **http** | **https**}] | **replace pattern-list** *list_num* [**protocol** {**all** | **http** | **https** | **rtsp**}] | **rewrite pattern-list** *list_num* [**protocol** {**all** | **http** | **https** | **rtsp**}] | **use-icap-service** *service-name* **pattern-list** *list_num* [**protocol** {**all** | **http** | **https**}] | **validate-url-signature pattern-list error-redirect-url** *url* | **exclude** {**all error-redirect-url** *url* **pattern-list** *num* [**protocol** {**all** | **http** | **rtmp** | **rtsp**}] | **client-ip error-redirect-url** *url* **pattern-list** *num* [**protocol** {**all** | **http** | **rtmp** | **rtsp**}] | **expiry-time error-redirect-url** *url* **pattern-list** *num* [**protocol** {**all** | **http** | **rtmp** | **rtsp**}] | **enable** | **pattern-list** *list_num* {**domain** *dn_regexp* | **group-type** {**and** | **or**} | **header-field** {**referer** *ref_regexp* | **src-ip** *s_ipaddress s_subnet* | **url-regex** *url_regexp* | **url-regsub** *url_regexp url_sub*}}}

no rule action {**allow pattern-list** *list_num* [**protocol** {**all** | **http** | **https** | **rtsp**}] | **block pattern-list** *list_num* [**protocol** {**all** | **http** | **https** | **rtsp**}] | **generate-url-signature** {**include-client-src-ip** | **key-id-owner** *key_id* {**key-id-number** *key_id_number*} {**pattern-list** *patterm_list_num*} [**protocol** {**all** | **http**}]} | **no-cache pattern-list** *list_num* [**protocol**{**all** | **http** | **https**}] | **redirect** *url* **pattern-list** *list_num* [**protocol** {**all** | **http** | **https** | **rtsp**}] | **refresh pattern-list** *list_num* [**protocol** {**all** | **http** | **https**}] | **replace pattern-list** *list_num* [**protocol** {**all** | **http** | **https** | **rtsp**}] | **rewrite pattern-list** *list_num* [**protocol** {**all** | **http** | **https** | **rtsp**}] | **use-icap-service** *service-name* **pattern-list** *list_num* [**protocol** {**all** | **http** | **https**}] | **validate-url-signature pattern-list error-redirect-url** *url* | **exclude** {**all error-redirect-url** *url* **pattern-list** *num* [**protocol** {**all** | **http** | **rtmp** | **rtsp**}] | **client-ip error-redirect-url** *url* **pattern-list** *num* [**protocol** {**all** | **http** | **rtmp** | **rtsp**}] | **expiry-time error-redirect-url** *url* **pattern-list** *num* [**protocol** {**all** | **http** | **rtmp** | **rtsp**}] | **enable** | **pattern-list** *list_num* {**domain** *dn_regexp* | **group-type** {**and** | **or**} | **header-field** {**referer** *ref_regexp* | **src-ip** *s_ipaddress s_subnet* | **url-regex** *url_regexp* | **url-regsub** *url_regexp url_sub*}}}

Syntax Description

action	Describes the action that the rule is to take.
allow	Allows the incoming request that matches the pattern list. This can be used in combination with block actions to allow selective types of requests. Allow does not carry any meaning as a standalone action.
pattern-list	Configures the pattern list.
list_num	Pattern list number. The range is from 1 to 512.
protocol	Specifies the protocol for which this rule is to be matched.
all	Matches this rule with all applicable protocols for this action.
protocol_type	Protocol types that support rule actions, namely, **http**, **https**, and **rtsp**. **Note** The term **http** traffic is used to see requests over HTTP including HTTP, FTP over HTTP, and HTTPS over HTTP. The Rules Template is not supported for FTP native requests.
enable	Enables rules processing on the SE.

pattern_type	Types of rule patterns that you can add to a pattern list.
allow	Allows the incoming request that matches the pattern list. This can be used in combination with block actions to allow selective types of requests. Allow does not carry any meaning as a standalone action.
http	Matches this rule with HTTP.
rtmp	Matches this rule with RTMP.
rtsp	Matches this rule with RTSP.
block	Blocks this request and allows all others.
generate-url-signature	Specifies that the SE generates a signed URL that is included in the autogenerated ASX file when content routing is in use and the pattern matches.
include-client-src-ip	Specifies the client IP to be included in the signed URL.
key-id-owner	Specifies the owner of the key which ranges from 1 to 32. The key is a shared secret string.
key_id	Owner of the key.
key-id-number	Specifies the identification number of the key. The range is from 1 to 16.
key_id_num	Identification number of the key.
pattern-list	Specifies the number of the pattern list. The range is from 1 to 512. Valid patterns are domain, url-regex, or dst-ip.
pattern_list_num	Specifies the number of the pattern list.
no-cache	Does not cache the object.
redirect	Redirects the request to the rewritten URL.
url	Redirect URL.
refresh	Revalidates the object with the web server.
replace	Replaces the text string in the object.
rewrite	Rewrites the original request as a specified URL and fetches the rewritten URL on a cache miss.
use-icap-service	Uses a specific ICAP server.
service_name	Service name used for handling a request through an ICAP server.
validate-url-signature	Validates a signed URL.
error-redirect-url	Specifies the error HTTP URL. **Note** This keyword is only supported for HTTP URLs.
exclude	Specifies what field in the URL signature must be validated.
all	Specifies both client-ip and expiry time fields are excluded in validation.
client-ip	Specifies that the client-ip field is excluded in validation.
domain-name	Specifies that the domain-name is excluded in validation.
expiry-time	Specifies that the expire-time field is excluded in validation.
domain	Specifies the regular expression to match the domain name.
dn_regexp	Regular expression to be matched with the domain name.
group-type	Specifies whether the pattern list is an AND or OR type.
and	Specifies an AND pattern to the pattern list.

or	Specifies an OR pattern to the pattern list.
header-field	Specifies the header field pattern of the request and substitute replacement pattern.
referer	Specifies the referer request header.
ref_regexp	Regular expression to be matched with the referer request header.
request-line	Specifies the request method line.
req_regexp	Regular expression to be matched with the request method line.
user-agent	Specifies the user agent request header.
ua_regexp	Regular expression to be matched with the User Agent request header.
src-ip	Specifies the source IP address of the request.
s_ipaddress	Source IP address of the request.
s_subnet	Source IP subnet mask.
url-regex	Specifies the regular expression to match a substring of the URL.
url_regexp	Regular expression to be matched with the URL string.
url-regsub	Sets the regular expression to match the URL and replacement pattern.
url_sub	URL string replacement pattern.

Command Defaults

The default is rule processing disabled.

The **group-type** pattern is OR by default.

Command Modes

Global configuration (config) mode.

Usage Guidelines

The Rules Template allows you to specify a set of rules, each clearly identified by an action and a pattern. The Rules Template allows you to configure an SE to use specific rules to filter HTTP, HTTPS, and RTSP traffic. A common use of this feature is to configure an SE to block the spread of Internet worms and viruses within an organization by checking whether a requested web page matches the pattern of a known Internet worm and if so then automatically blocking the request.

If you have enabled rules processing on an SE (enabled the Rules Template feature on the SE and configured rules for the SE), the SE checks each incoming client request to determine if a rule pattern matches the requested content. If a rule pattern matches the given request, the SE uses the specified action (policy) to handle this incoming traffic.

The SE can match incoming requests against the following:

- Patterns in the IP address of the client requesting the content (source IP address), including the IP address, the network mask, and the port list
- Patterns in the IP address of the origin web or media server (destination IP addresses), including the IP address, the network mask, and the port list
- Regular expression of the URL
- Regular expression of the domain portion of the URL
- MIME types of the web object that the client is requesting
- Regular expressions symbolizing domain names

- Headers that are sent in the request, including the following:
  - User-agent of the request, which indicates which client software is issuing the request
  - Referer, which indicates the web page from which the browser jumped to this link
  - Request line, which indicates the request line itself

Note The regsub attribute supports regular expressions, but only one substitution can be defined. Multiple substitutions are not supported. Also, only one url-regsub pattern list is supported. Multiple substitutions for the same pattern list are not supported.

You can apply the policies defined in the Rules Template to HTTP (including FTP over HTTP) and HTTPS and to RTSP for streaming media objects. Policies that can be applied include the following:

- Allowing a request to be completed
- Blocking the request
- Overriding the HTTP response header and caching the object
- Caching the object depending on the HTTP response header
- Bypassing authentication for the request
- Replacing the text string
- Not caching an object
- Bypassing an upstream proxy for the request
- Redirecting the request to a different URL
- Revalidating the object with the origin server
- Rewriting the URL
- No URL filtering for the specified HTTP and HTTPS requests
- Using a specific ICAP server
- Using a specific upstream proxy
- Using a specific server for the request

Note To enter a question mark (?) in a rule regular expression from the command-line interface, use the escape character followed by a question mark (?). Use of the escape sequence prevents the command-line interface from displaying context-sensitive help.

Supported Rule Actions per Protocol

For RTSP, the redirect rule actions are supported for RTSP requests from RealMedia players. These two rule actions are not supported for RTSP requests from Windows Media Players. For example, Windows Media Services 9 (WMS 9) supports the block, rewrite, and allow rule actions for RTSP requests, but does not support the redirect rule actions for RTSP requests.

WMT supports all the rule action types—allow, block, no-cache, redirect, refresh, replace, rewrite, validate-url-signature, and generate-url-signature. RTMP and Movie Streamer only support allow, block, and validate-url-signature.

Note If the **rule action generate-url-signature** command with the parameter **include-client-src-ip key-id-owner 3 key-id-number 3 pattern-list 2** is entered, with and without protocol parameters, the "rule entry is duplicate" message is displayed. If the protocol is not specified in that particular pattern list, all protocols are accepted.

This command removes the trailing "protocol all" when it displays in the running-config. All service rule-related commands have this functionality. Also, the **rule action allow pattern-list 1 ?** command does not have a help message indicating "protocol all" is the default value if it is omitted.

Supported Action and Pattern Combinations

Not all actions support all patterns for request matching because some patterns do not make sense for some actions.

Understanding Actions and Patterns

A *rule* is specified by an action and a pattern list. An action is performed on a request if this request matches the pattern list specified in the **rule pattern-list** command.

An *action* is something that the SE performs when processing a request; for instance, an action could be blocking the request, using an alternative proxy, and so forth.

A *pattern list* defines the limits of a request; for instance, a pattern list may specify that the source IP address falls in the subnet range 172.16.*.*.

Rules can be dynamically added, displayed, or deleted from the SE. The rules are preserved across reboots because they are written into persistent storage, such as NVRAM, using the appropriate CLI commands or the CDSM GUI. Only the system resources limit the number of rules that the SE can support. Because rules consume resources, the more rules that you define can greatly impact how the SE performs.

Note The number of actions is limited only by available resources. The maximum number of pattern lists is 512. The maximum number of patterns per action is 128. A single pattern list can contain up to 128 patterns of a particular pattern type.

Actions

The Rules Template supports the following types of actions:

- **Allow**—Allows incoming requests that match the pattern list.

  This rule action can be used in combination with block actions to allow selective types of requests. Allow does not carry any meaning as a standalone action.

- **Block**—Blocks this request and allows all others.
- **No-cache**—Does not cache this object.
- **Redirect**—Redirects the original request to a specified URL. Redirect is relevant to the RADIUS server only if the RADIUS server has been configured for **redirect**.
- **Refresh**—For a cache hit, forces an object freshness check with the server.
- **Replace**—Replaces the text string in the object.
- **Rewrite**—Rewrites the original request as a specified URL. The SE searches for the rewritten URL in the cache, and then on a cache miss, fetches the rewritten URL and returns the object transparently to the client. You should use a **redirect** rule instead of a **rewrite** rule because of possible

performance impacts. The reason for the performance impact is that, for a **redirect** rule, the SE sends a 302 (Found) message to the client with the new redirect URL. The client issues a separate request to the redirected URL. However, for a **rewrite** action, the original request URL is rewritten as the specified URL. The URL rewrite could change the domain name of the URL, which necessitates a Domain Name Server (DNS) lookup to find the destination IP address of the new rewritten server to which the request must be sent.

- **Use-icap-service**—Uses a specified ICAP server.
- **Validate-url-signature**—Validates a signed URL.

Actions can be applied to specific protocols or to a set of protocols. If no protocol is configured, then the specified action is taken for all the traffic that goes through the SE.

Execution Order of Rule Actions

The order in which the rule actions are executed is different between the Web Engine and the other protocol engines (Windows Media Streaming, Movie Streamer, and Flash Media Streaming).

Note For the Web Engine, the Service Rule file must be used if service rules are to be configured. This is done though the CDSM, not the CLI. For more information, see Appendix F "Creating Service Rule Files" of the *Cisco Internet Streamer CDS 3.0 Software Configuration Guide*.

Note Configuring Service Rules for Flash Media Streaming is no longer done through the CLI; it is done through the Authorization Server Rules plug-in. See the "Configuring Service Rules" section in the *Cisco Internet Streamer CDS 3.0 Software Configuration Guide*.

Note When configuring service rules, you must configure the same service rules on all SEs participating in a delivery service in order 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.

Web Engine Rule Action Order

The order in which the rule actions are executed for the Web Engine is as follows:

1. block or allow

Note The allow and block actions carry the same precedence. The order of execution depends on the order of configuration between allow and block actions. Other actions always take precedence over allow.

2. redirect (before cache lookup)
3. rewrite (before cache lookup)
4. use-icap-service
5. generate-url-signature
6. validate-url-signature
7. refresh (after cache lookup, in the case of cache hit)
8. no-cache

All Other Protocol Engine Rule Action Order

The order in which the rule actions are executed for the other protocol engines is the order in which they were configured, except for the validate-url-signature action. If the rule pattern associated with the validate-url-signature action is matched, regardless of the configuration order the rules, the validate-url-signature action is performed before any other action.

1. validate-url-signature
2. block or allow

Note The allow and block actions carry the same precedence. The order of execution depends on the order of configuration between allow and block actions. Other actions always take precedence over allow.

3. redirect (before cache lookup)
4. rewrite (before cache lookup)

Patterns

The Rules Template supports the following pattern types:

- **Domain**—Matches the domain name in the URL or the Host header against a regular expression. For example, .*ibm.* matches any domain name that contains the ibm substring. The \.foo\.com$ domain name matches any domain name that ends with the .foo.com substring.

  Note In regular expression syntax, the dollar sign ($) metacharacter directs that a match is made only when the pattern is found at the end of a line.

- **Group-type**—Specifies whether the pattern list is an AND or OR type. The default is OR. Following are the four patterns of expected behavior:
  - **Pattern 1**

    rule pattern-list 22 group-type and

    rule pattern-list 22 url-regsub 10 airforce

    rule pattern-list 22 url-regsub wma wmv

    rule pattern-list 23 url-regsub 10 airforce

    rule pattern-list 23 url-regsub wma wmv
  - **Pattern 2**

    rule pattern-list 22 group-type and

    rule pattern-list 22 url-regsub 10 airforce

    rule pattern-list 23 url-regsub wma wmv
  - **Pattern 3**

    rule pattern-list 22 group-type or

    rule pattern-list 22 url-regsub 10 airforce

    rule pattern-list 22 url-regsub wma wmv

    rule pattern-list 23 url-regsub 10 airforce

    rule pattern-list 23 url-regsub wma wmv

– **Pattern 4**

rule pattern-list 22 group-type or

rule pattern-list 22 url-regsub 10 airforce

rule pattern-list 23 url-regsub wma wmv

Note The rules are that when AND is specified for a pattern-list ALL the conditions satisfy. When OR is specified, ANY of the condition are matched.

- **Src-ip**—Matches the request's source IP address and netmask. Specify an IP address and a netmask.
- **URL-regex**—Matches the URL against a regular expression. The match is case insensitive. Specify a regular expression.
- **Header-field**—Matches the header field pattern of the request.

  Request header field patterns **referer**, **request-line**, and **user-agent** are supported for the actions **block**, **redirect**, and **rewrite**. The **referer** pattern is matched against the Referer header in the request, the **request-line** pattern is matched against the first line of the request, and the **user-agent** pattern is matched against the User-Agent header in the request.
- **URL-regsub**—Matches the URL against a regular expression to form a new URL per pattern substitution specification for the **rewrite** and **redirect** actions. The match is case insensitive. The valid substitution index range is from 1 to 9.

If an empty string is given as a replacement pattern, the Referer header is stripped. Stripping of the Referer header occurs in the **user-agent** pattern.

Multiple patterns can be entered on the same pattern list. If any of them matches the incoming request, the corresponding action is taken.

Multiple patterns for the same pattern list must be entered on different lines.

Rules Template Processing Considerations

Actions and patterns have a predefined order of execution. A group of rules with the same action is always executed either before or after another group of rules with a different action. The **block**, **rewrite**, and **redirect** rule actions support the following additional patterns: **request-line**, **referer**, and **user-agent** regular expressions. The **request-line** regular expression matches the first line of the request. The **user-agent** regular expression matches the User-Agent header value of the request. The **referer** regular expression matches the Referer header value of the request. The order is not affected by the order in which the rules are entered using CLI commands.

Allow and **block** carry the same precedence. The order of execution depends on the order of configuration between **allow** and **block** actions. Other actions always take precedence over **allow**.

Among rules of the same action, a predefined execution order exists among the rule patterns, which means that within a group of rules of the same action, one group of rules with the same pattern is always executed either before or after another group of rules with a different pattern.

Among all rules of the same action and of the same rules pattern, the rules are evaluated in a Last-Entered-First-Examined fashion (the reverse of the order in which the rules were entered). This order is not affected by the order in which the rules are entered using CLI commands.

Most actions do not have any parameters.

Service Rules for URLs

There are three cases for service rules:

- If **allow** rules are configured, then it is an implicit deny.

  For example, if all URL requests that match HTML are blocked, implicitly, all requests that match other URL requests are allowed.

- If **deny** rules are configured then it is implicit allow.

  If all URL requests that match WMV are allowed, implicitly, all request that match other URL requests are blocked.

- If both **allow** and **deny** are configured, then it is an implicit allow.

  If both of the above rules are configured, then HTML URL requests are blocked, and all other URL requests are allowed.

Examples

The following example shows that the SE is configured to replace the internal.domain.com string in a request to the server named dummy:

```
ServiceEngine(config)#  rule action rewrite header-field referer internal.domain.com dummy
```

The following example shows that if an empty string is given as a replacement pattern, then the referer header is stripped. This rule states that all requests, which have a referer header that indicates a corporate internal server in ABCBigCorp, strip the referer field so that the outside web server does not see the name of the corporate internal server.

```
ServiceEngine(config)#  rule action rewrite header-field referer internal.abcbigcorp.com
""
```

The following example shows that the **rule pattern-list** command is configured to add a pattern to an existing pattern list to perform an action to be defined on destination IP address 172.16.25.25 using the dst-ip pattern:

```
ServiceEngine# show rule pattern-list 10 all
Rules Template Configuration
----------------------------
Rule Processing Enabled

Pattern-Lists :

rule pattern-list 11 dst-ip 172.16.25.25 255.255.255.0
rule pattern-list 11 domain foo.com
```

The following example shows that the **rule action block** command is configured and associated with an existing pattern list:

```
ServiceEngine(config)# rule action block pattern-list 10 protocol all
ServiceEngine# show rule action block
Rules Template Configuration
----------------------------
Rule Processing Enabled

Actions :

rule action block pattern-list 10 protocol all
```

The following example shows that the **rule action block** command is configured and associated with an existing pattern list, which lists as its pattern the domain yahoo.com:

```
ServiceEngine(config)# rule pattern-list 10 domain yahoo.com
ServiceEngine# show rule pattern-list 10 all
Rules Template Configuration
```

```
---------------------------
Rule Processing Enabled

Pattern-Lists :

rule pattern-list 10 domain yahoo.com
ServiceEngine(config)# rule action block pattern-list 10 protocol all
```

In this example, the request (using HTTP) to yahoo.com was denied three times.

The following example shows that the **rule action block** command (action) blocks all patterns specified with the **rule pattern-list 12** command:

```
ServiceEngine(config)# rule pattern-list 12 domain \.foo.com
ServiceEngine(config)# rule action block pattern-list 12
ServiceEngine(config)#
```

The following example prevents caching of requests that match a URL request that contains the *cgi-bin* string:

```
ServiceEngine(config)# rule pattern-list 13 url-regex \.*cgi-bin.*
ServiceEngine(config)# rule action no-cache pattern-list 13
ServiceEngine(config)#
```

The actions that are to be taken by the rules are configured through the **rule action** commands. Patterns that are to be matched to a particular pattern that you specify are configured through **rule pattern-list** commands.

The following example shows how patterns use AND by configuring patterns with the same pattern list number and applying that pattern list to an action:

```
ServiceEngine(config)# rule action block pattern-list 1
ServiceEngine(config)# rule pattern-list 1 url-regex yahoo
ServiceEngine(config)# rule pattern-list 1 dst-port 80
```

Other options of the **rule** command work similarly to the preceding examples.

The following example redirects a request for old-domain-name that has been changed to new-domain-name:

```
Cache(config)# rule action redirect http://old-domain-name/ pattern-list 1 protocol http
Cache(config)# rule pattern-list 1 url-regsub http://old-domain-name/
http://new-domain-name/
```

The following example redirects requests from an IETF site to a site that is locally mirrored:

```
Cache(config)# rule action redirect http://www.ietf.org/rfc/(.*) pattern-list 2 protocol
http
```

The following example shows that if the request URL is http://www.ietf.org/rfc/rfc1111.txt, the SE rewrites the URL as http://wwwin-eng.cisco.com/RFC/RFC/rfc1111.txt and sends a 302 Temporary Redirect response with the rewritten URL in the Location header to the client. The browser automatically starts a request to the rewritten URL.

```
Cache(config)# rule pattern-list 2 url-regsub http://www.ietf.org/rfc/(.*)
http://wwwin-eng.cisco.com/RFC/RFC/\1
```

The following example redirects all requests for linux.org to a local server in India that is closer to where the SE is located:

```
Cache(config)# rule action redirect http://linux.org/(.*) pattern-list 3 protocol http
```

The following example shows that two URLs are to be matched if the pattern is **url-regsub**. If the URLs that are given in the action configuration are invalid, a warning is displayed during the configuration of this rule. The action URL is taken when the header field patterns are configured.

```
Cache(config)# rule pattern-list 3 url-regsub http://linux.org/(.*) http://linux.org.in/\1
```

The following example bypasses requests with cisco.com as the domain from URL filtering:

```
ServiceEngine(config)# rule action no-url-filtering pattern-list 6 protocol all
ServiceEngine(config)# rule pattern-list 6 domain cisco.com
```

The following example covers both uppercase and lowercase expressions of MP4 files:

```
ServiceEngine(config)# rule pattern-list 2 url-regex http://(.*.)cdsis.com/(.*.)[mM]
[pP]4(.*)
```

Related Commands

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.
show rule	Displays rules configuration information.

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 sysfs file in the current directory.
file_name	Name of the script file.

Command 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 CDSM:

service csm restart

On the SE:

service {**acquisition restart | csm restart | distribution restart | flash-media-streaming restart | ms restart | rtspg restart | web-engine restart | wmt restart**}

On the SR:

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

Syntax Description

acquisition	Specifies Acquisition services.
restart	Restarts the specified services.
csm	Specifies CMS services.
distribution	Specifies Distribution services.
flash-media-streaming	Specifies Flash Media Streaming services.
ms	Specifies Movie Streamer services.
rtspg	Specifies RTSP Gateway services.
service-router	Specifies Service Router services.
web-engine	Specifies Web Engine services.
wmt	Specifies Windows Media services.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to start acquisition service:

```
ServiceEngine# service acquisition restart
The service acquirer 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* | **fms** *num* | **kmemory** *num* | **memory** *num* | **wmt** *num* | **nic** *num*} | **sample-period** {**all** *num* | **cpu** *num* | **disk** *num* | **fms** *num* | **kmemory** *num* | **memory** *num* | **movie-streamer** *num* | **nic** *num* | **wmt** *num*} | **threshold** {**augmentation** *num* | **burstcnt** *num* | **cpu** *num* | **disk** *num* | **faildisk** *num* | **fms** *num* | **kmemory** *num* | **memory** *num* | **movie-streamer** *num* |**nic** *num* | **wmt** *num*} | **transaction-log enable** | **type** {**all** | **cpu** | **disk** | **fms** | **kmemory** | **memory**| **movie-streamer** | **nic** | **wmt**}}}

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

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 CDSM:

service-router {**access-policy enable** | **content-based-routing** {**enable** | **redundant** *num*} | **lastresort** {**domain** *name* {**allow all** | **alternate** *name port_num*} | **error-domain** *name* **error-file** *port_num* | **translator** *ip_address port_num*} | **location-based-routing** {**enable** | **location-cache timeout** *num*} | **proximity-based-routing** {**enable** | **proximity-cache timeout** *num* | **proximity-server** *ip_address* **password** *password*} | **redirect-burst-control** {**enable** | **rate** *num*} | **redirect-mode** {**dns-redirect** {**all** | **domain** *domain*} | **ip-redirect**} | **service-monitor** {**augmentation-alarm enable** | **number-of-samples** {**all** *num* | **cpu** *num* | **disk** *num* | **kmemory** *num* | **memory** *num*}} | **subscribe domain** *domain* | **threshold** {**augmentation** *num* | **cpu** *num* | **disk** *num* | **kmemory** *num* | **memory** *num* | **transaction-log enable**}}

no service-router {**access-policy enable** | **content-based-routing** {**enable** | **redundant** *num*} | **lastresort** {**domain** *name* {**allow all** | **alternate** *name port_num*} | **error-domain** *name* **error-file** *port_num* | **translator** *ip_address port_num*} | **location-based-routing** {**enable** | **location-cache timeout** *num*} | **proximity-based-routing** {**enable** | **proximity-cache timeout** *num* | **proximity-server** *ip_address* **password** *password*} | **redirect-burst-control** {**enable** |

rate *num*} | **redirect-mode** {**dns-redirect** {**all** | **domain** *domain*} | **ip-redirect**} | **service-monitor** {**augmentation-alarm enable** | **number-of-samples** {**all** *num* | **cpu** *num* | **disk** *num* | **kmemory** *num* | **memory** *num*}} | **subscribe domain** *domain* | **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.
fms	Sets the FMS[1] monitor type.
kmemory	Sets the monitor kernel memory type.
memory	Sets the monitor memory type.
movie-streamer	Monitors the Movie Streamer stream count.
wmt	Sets the WMT[2] monitor 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.
movie-streamer	Sets the Movie Streamer monitor type.
type	Configures the type to be monitored.
access-policy	Configures the service-router access-policy.
enable	Enables the access-policy.
enable	Enables the CDN Selector.

content-based-routing	Configures content based routing.
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 server.
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.
location-based-routing	Configures location-based routing.
enable	Enables location-based routing.
location-cache	Configures the location cache.
timeout	Configures the location cache timeout.
num	Location cache timeout in seconds (0 to864000).
proximity-based-routing	Configures proximity-based routing.
enable	Enables proximity-based routing.
proximity-cache	Configures proximity cache.
timeout	Configures proximity cache timeout.
num	Proximity cache timeout, in seconds. The range is from 1 to 86400.
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.
redirect-mode	Enables the redirect mode. The redirect mode is disabled by default.

dns-redirect	Sets the redirect mode to DNS-based redirection. **Note** The TTL for the DNS proxy requests is one second. A one-second TTL ensures that the DNS proxy keeps sending requests to the Request Routing Engine, which in turn causes the Request Routing Engine to determine the best Service Engine at that point in time, and not to redirect the request to the same SE.
all	Enables the DNS-based redirection for all domains.
domain	Enables the DNS-based redirection for a specific domain.
domain	Name of the domain.
ip-redirect	Sets the redirect mode to IP-based redirection.
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.
subscribe	Configures the domains to which the service router should be subscribed.
domain	Configures the domain.
domain	Specifies the domain name.
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.

1. FMS = Flash Media Server
2. WMT = Windows Media Technology

Command Defaults

keepalive-interval: 2

redundant copies: 1

dns-ttl: 60

burstcnt: 1

location cache timeout: 691200 seconds (8 days)

content-based-routing: disabled

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 server.

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 CDSMs. 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 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.

Location-Based Routing

The Geo-Location servers were introduced with the location-based routing method. Once you enable location-based routing, you must specify the Geo-Location servers.

The Authorization Service uses an XML file to allow or deny client requests based on the client's IP address or geographic location. The country, state, and city names in the Authorization XML file must match what is used by the Geo-Location server and the names are case sensitive.

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 server), the request cannot be served unless the origin server 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 cds-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 cds-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 cds-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 server.

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, the Flash Media Streaming engine, and the Movie Streamer 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

Domain Subscription

The **service-router subscribe domain** command allows us to specify domains to which the service router should be subscribed. By default the service-router takes all the domains specified in the CDSM. Even if you configure only one domain subscription through this command, the SR takes the list of domains subscribed through the CLI to be the complete list.

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 2-12 describes the fields for the Service Router transaction log.

Table 2-12 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.
routing-method	Routing method chosen. The routing-method field has the following possible values: • Last-Resort • Network • Proximity • Zero-Network • Geo-Location
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 CDSM.
- *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 2-13 describes the fields for the Service Monitor transaction log on an SE.

Table 2-13 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.	–

Table 2-13 SE Service Monitor Transaction Log Fields (continued)

Field	Sample Output	Description	Corresponding CLI Command
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.	–
ms_threshold_exceeded	–	Boolean value to indicate if the Movie Streamer threshold has been exceeded.	**show service-router service-monitor** Services status—MS—Threshold
ms_augment_threshold_ Exceeded	–	Boolean value to indicate if Movie Streamer augmentation alarm threshold has been exceeded.	–
ms_stopped	–	Boolean value to indicate if the Movie Streamer protocol engine has stopped.	**show service-router service-monitor** Services status—MS—Stopped
ms_rtsp_sessions_ count	–	Total Movie Streamer RTSP session count (aggregate value).	**show statistics movie-streamer all** Total RTSP sessions
ms_rtp_sessions_count	–	Total Movie Streamer RTP session count (aggregate value).	**show statistics movie-streamer all** Total RTP connections
fms_threshold_ exceeded	N	Boolean value to indicate if threshold is exceeded.	**show service-router service-monitor** Services status—FMS—Threshold
fms_augment_threshold_ exceeded	N	Boolean value to indicate if Flash Media Streaming augmentation alarm threshold has been exceeded.	–
fms_stopped	N	Boolean value to indicate if Flash Media Streaming has stopped.	**show service-router service-monitor** Services status—FMS—Stopped
fms_connections_count	2	Total Flash Media Streaming connection count (aggregate value).	**show statistics flash-media-streaming** Connections—Total

Table 2-13 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 server.	**show statistics web-engine detail** Web-Engine Detail Statistics—Total HTTP Connection
wmt_threshold_ exceeded	N	Boolean value to indicate if Windows Media Streaming threshold has been exceeded.	**show service-router service-monitor** Services status—WMT—Threshold
wmt_augment _threshold_exceeded	N	Boolean value to indicate if the Windows Media Streaming augmentation alarm threshold has been exceeded.	–
wmt_stopped	Y	Boolean value to indicate if Windows Media Streaming has stopped.	**show service-router service-monitor** Services status—WMT—Stopped
wmt_ml_cpu_percentage	21	Percentage of the CPU used by the WMT_ML process.	–
wmt_ml_mem (bytes)	32456	Memory (in bytes) used by WMT_ML process	–
wmt_core_cpu_ percentage	21	Percentage of the CPU used by the WMT_Core process.	–
wmt_core_mem (bytes)	32456	Memory (in bytes) used by the WMT_Core process.	–
wmt_unicast_sessions	22	Number of current concurrent unicast client sessions.	**show statistics wmt usage** Concurrent Unicast Client Sessions—Current
wmt_remote_sessions	24	Number of current concurrent remote server sessions.	**show statistics wmt usage** Concurrent Remote Server Sessions

Table 2-13 SE Service Monitor Transaction Log Fields (continued)

Field	Sample Output	Description	Corresponding CLI Command
wmt_live_requests	21	Total count of Windows Media Streaming live requests (Aggregate value).	**show statistics wmt requests** By Type of Content—Live content
wmt_vod_requests	22	Total count of Windows Media Streaming VOD requests (Aggregate value).	**show statistics wmt requests** By Type of Content—On-Demand Content
wmt_http_requests	11	Total count of Windows Media Streaming HTTP requests (Aggregate value).	**show statistics wmt requests** By Transport Protocol—HTTP
wmt_rtsp_requests	8	Total count of Windows Media Streaming RTSP requests (Aggregate value).	**show statistics wmt requests** By Transport Protocol—RTSPT/RTSPU
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 2-14 describes the fields for the Service Monitor transaction log on a SR.

Table 2-14 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
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.	–

Table 2-14 SR Service Monitor Transaction Log Fields (continued)

Field	Sample Output	Description	Corresponding CLI Command
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 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, 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 enable crossdomain support:

```
ServiceEngine(config)# service-router access-policy enable
```

The following example shows how to disable crossdomain support:

```
ServiceEngine(config)# no service-router access-policy enable
```

The following example shows how to configure Proximity Engine cache on an SR:

```
ServiceRouter(config)# proximity engine enable
Starting Proximity Engine....
Proximity Engine Started.

ServiceRouter(config)# service-router proximity-based-routing proximity-server 127.0.0.1

ServiceRouter(config)# service-router proximity-based-routing proximity-cache timeout 600

ServiceRouter(config)# service-router proximity-based-routing enable
Please ensure you have purchased License for this advanced feature
ServiceRouter(config)# end
```

The following example shows how to enable DNS-based redirection with the cdsfms.com domain as the domain used to redirect all client requests to:

```
ServiceRouter(config)# service-router redirect-mode dns-redirect domain cdsfms.com
```

The following example shows how to display information about the redirect mode by entering the **show service-router redirect-mode** command:

```
ServiceRouter# show service-router redirect-mode
    ip-redirect is enabled
    dns-redirect domain fms.cds.com
    dns-redirect domain cds.com
    dns-redirect domain abc.com
    dns-redirect domain cdsfms.com
```

The following example shows how to subscribe the SR to a domain named test3.com:

```
    ServiceRouter(config)# service-router subscribe domain test3.com
    ServiceRouter(config)#
```

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        :                 2
  HTTP Requests (normal) :                 0
  HTTP Requests (ASX)    :                 0
  RTSP Requests          :                 0
  RTMP Requests          :                 0
  DNS Requests           :                 2

Requests Served          :                 0
  HTTP Requests Served   :                 0

Requests Redirected      :                 1
  HTTP 302 Redirects     :                 0
  ASX Redirects          :                 0
  RTSP redirects         :                 0
  RTMP redirects         :                 0
  DNS redirects          :                 1

Requests Overflowed      :                 1
  HTTP 302 Redirects     :                 0
  ASX Redirects          :                 0
  RTSP redirects         :                 0
  RTMP redirects         :                 0
  DNS redirects          :                 1

Requests Not Redirected  :                 0
  No SE Covering Client  :                 0
  Unknown Content Origin :                 0
  Route Table Locked     :                 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 cds.com translator 171.XX.XX.XXX
ServiceRouter(config)# service-router last-resort domain cdsis.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 cds.com translator 171.XX.XX.XXX
Domain cdsis.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.

Command Defaults

None

Command Modes

EXEC configuration mode.

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 Internet Streamer CDS 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 aaa

To display the accounting, authentication, and authorization configuration, use the **show aaa** command in EXEC configuration mode.

show aaa {**commands** [**accounting** | **authorization**] | **enable** [**authentication**] | **exec** [**accounting** | **authorization**] | **login** [**authentication**] | **system** [**accounting** | **authorization**]}

Syntax Description

commands	Configures exec (shell) commands.
accounting	(Optional) Displays the Accounting configuration.
authorization	(Optional) Displays the Authorization configuration.
enable	Configures enable.
authentication	(Optional) Displays Authentication configuration.
exec	Configures starting an exec (shell).
login	Configures the user's login to the system.
system	Configures system events.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-15 describes the fields shown in the **show aaa commands** command display.

Table 2-15 show aaa commands Field Descriptions

Field	Description
Configuration commands Authorization	Authorization through Tacacs+ for configuration mode commands is enabled or disabled.
Commands on console Line Authorization	Authorization through TACACS+ for all commands issued from console line is enabled or disabled.
Exec commands Authorization: Normal Users	
Exec commands Authorization: Super Users	
Tacacs+	Authorization through Tacacs+ for exec (shell) commands issued by normal users is enabled or disabled.

Table 2-15 show aaa commands Field Descriptions (continued)

Field	Description
Exec Commands Accounting: Normal Users	
Tacacs+	Authorization through Tacacs+ for exec (shell) commands issued by super users is enabled or disabled.
Exec Commands Accounting: Super Users	
Tacacs+	Accounting through Tacacs+ for exec (shell) commands issued by normal users is enabled or disabled.

Table 2-16 describes the fields shown in the **show aaa enable** command display.

Table 2-16 show aaa enable Field Descriptions

Field	Description
Enable Authentication: All Users	
Enable	Authentication through local configured Enable password for enable is enabled or disabled.
Radius	Authentication through Radius for enable is enabled or disabled.
Tacacs+	Authentication through Tacacs+ for enable is enabled or disabled.

Table 2-17 describes the fields shown in the **show aaa exec** command display.

Table 2-17 show aaa exec Field Descriptions

Field	Description
Starting exec Authorization:	
Local	Authorization through local for starting exec is enabled or disabled.
Radius	Authorization through Radius for starting exec is enabled or disabled.
Tacacs+	Authorization through Tacacs+ for starting exec is enabled or disabled.
Exec events Accounting	
Tacacs+	Accounting through Tacacs+ for exec event is enabled or disabled.

Table 2-18 describes the fields shown in the **show aaa login** command display.

Table 2-18 show aaa login Field Descriptions

Field	Description
Login Authentication	
Local	Authentication through local configured user password for login is enabled or disabled.
Radius	Authentication through Radius for login is enabled or disabled.
Tacacs+	Authentication through Tacacs+ for login is enabled or disabled.

Table 2-19 describes the fields shown in the **show aaa system** command display.

Table 2-19 show aaa system Field Descriptions

Field	Description
System events Accounting	
Tacacs+	Accounting through Tacacs+ for system event is enabled or disabled.

Related Commands

Command	Description
aaa	Configures accounting, authentication and authorization methods.
show aaa	Displays the accounting, authentication and authorization configuration.
show statistics aaa	Displays accounting, authentication and authorization statistics.

show access-lists 300

To display the access control list (ACL) configuration, use the **show access-lists 300** command in EXEC configuration mode.

show access-lists 300

Syntax Description

This command has no arguments or keywords**.**

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-20 describes the fields shown in the **show access-lists 300** display.

Table 2-20 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 acquirer

To display the acquirer information and progress of content acquisition for a specified channel number or name, use the **show acquirer** command in EXEC configuration mode.

show acquirer [**delivery-service** {**delivery-service-id** *delivery_service_id* | **delivery-service-name** *delivery_service_name*} | **progress** {**delivery-service-id** *delivery_service_id* | **delivery-service-name** *delivery_service_name*} | **proxy authentication**]

Syntax Description

delivery-service	(Optional) Displays acquirer information for the delivery service.
delivery-service-id	Displays the ID for the delivery service.
delivery_service_id	Delivery service ID.
delivery-service-name	Displays the name for the delivery service.
delivery_service_name	Delivery service name.
progress	(Optional) Displays the acquisition progress for the specified channel.
proxy	(Optional) Displays the proxy information for the acquirer.
authentication	(Optional) Displays the proxy authentication details for the acquirer.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **show acquirer progress** command displays information for all channels for which the SE is the Content Acquirer. It displays the number of acquired objects in relation to the total number of objects for both a single item or crawler jobs. When an acquisition is in progress, it displays the number of data bytes currently being downloaded in relation to the total size of the object and its URL. The **show acquirer progress** command also displays information about the authentication that allows the acquirer to access content through a transparent or nontransparent proxy server.

The **show acquirer proxy authentication** command displays the proxy authentication configuration for the acquirer if you have enabled content acquisition through a proxy server and proxy authentication is configured. Use the **acquirer proxy authentication outgoing** command in Global configuration mode to configure authentication when you enable content acquisition through a proxy server. You must first configure the proxy host and the port using the **http proxy outgoing host** command in Global configuration mode.

When you enable content acquisition through a proxy server, you can provide the proxy configuration and proxy authentication information in the manifest file. If the proxy and proxy authentication are configured in the manifest file, the **show acquirer proxy authentication** command does not display any proxy details.

The **show acquirer progress** command in EXEC configuration mode displays the progress of the acquirer for a specified channel. If a specific channel is not mentioned, the display shows the progress for all the channels for which the SE is the root.

Table 2-21 describes the fields shown in the **show acquirer progress** display.

Table 2-21 show acquirer progress Field Descriptions

Field	Description
Channel-id	Numerical identifier for the channel.
Channel-Name	Name for the channel.
Acquired Single Items	Total number of single items completed out of all the single items specified in the manifest. For example, 200/301 shows that all 200 items out of a total of 301 items have been acquired.
Acquired Crawl Items	Total number of links with crawling completed out of the total crawlable items for each crawling task specified in the manifest, along with the starting URL.
Download Size (Bytes)	Current URL fetched by the acquirer for the channel, if applicable, along with the file size details.

The following example shows the output from the **show acquirer proxy authentication** command when there are no proxies configured using the **acquirer proxy authentication** command in Global configuration mode:

```
ServiceEngine# show acquirer proxy authentication
No proxy authentication information configured
```

The following example shows the output from the **show acquirer proxy authentication** command after configuring the proxy using the **acquirer proxy authentication** command in Global configuration mode:

```
ServiceEngine# show acquirer proxy authentication
acquirer proxy authentication outgoing 172.28.225.29 8080 admin password **** My-Domain
basic-auth-disable
acquirer proxy authentication transparent admin password **** My-Domain basic-auth-disable
```

Related Commands

Command	Description
acquirer (Global configuration)	Provides authentication when the acquirer obtains content through a proxy server.
http	Configures HTTP-related parameters.
show statistics acquirer	Displays SE acquirer channel statistics.

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.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The Node Health Manager enables CDS 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 Internet Streamer CDS software alarms.

The Internet Streamer CDS software uses SNMP to report error conditions by generating SNMP traps. In the Internet Streamer CDS software, the following SE applications can generate an Internet Streamer CDS 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 Internet Streamer CDS 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 Internet Streamer CDS 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 Internet Streamer CDS software on the SE. The Internet Streamer CDS 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, the Flash Media Streaming engine, and the Movie Streamer engine.

Table 2-22 describes the fields shown in the **show alarms history** display.

Table 2-22 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 2-23 describes the fields shown in the **show alarms status** display.

Table 2-23 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 SE to send 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.

Command 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 2-24 describes the fields shown in the **show arp** display.

Table 2-24 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.

Command Defaults

None

Command Modes

EXEC configuration mode.

Related Commands

Command	Description
aaa	Specifies accounting, authentication and authorization methods.
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.

show authsvr

To display the status of the Authorization server, use the **show authsvr** command in EXEC configuration mode.

show authsvr [**unknown-server | location-server**]

Syntax Description

unknown-server	(Optional) Shows the allow and deny rule for unknown configured servers or domains.
location-server	(Optional) Shows the Location server configuration. It includes both primary and secondary geo location server information.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to display the status of the Authorization server:

```
ServiceEngine# show authsvr
Authserver is Enabled
```

The following example shows the status of the Location server:

```
ServiceEngine# show authsvr location-server
        Primary geo location server 4.0.1.3 7000
        Secondary geo location server 171.71.50.140 7000
```

Related Commands

Command	Description
authsvr	Enables and configures the Authorization server.

show bandwidth

To display the bandwidth allocated to a particular device, use the **show bandwidth** command in EXEC configuration mode.

show bandwidth [**flash-media-streaming** | **movie-streamer** | **wmt**]

Syntax Description

flash-media-streaming	(Optional) Displays the Flash Media Streaming bandwidth settings.
movie-streamer	(Optional) Displays the Movie Streamer bandwidth settings.
wmt	(Optional) Displays Windows Media Technology (WMT) bandwidth settings.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-25 describes the fields shown in the **show bandwidth** display.

Table 2-25 show bandwidth Field Descriptions

Field	Description
Module	Types of application servers for which bandwidth allocation is displayed: • **wmt incoming** is for incoming WMT streaming content requests from end users. • **wmt outgoing** is for outgoing WMT media from SEs. • **movie-streamer incoming** is for incoming Movie Streamer content requests from end users. • **movie-streamer outgoing** is for outgoing Movie Streamer media from SEs. • **flash-media-streaming** is for Flash Media Streaming.
Bandwidth Kbps	Maximum amount of bandwidth that you want allowed in kbps[1] for a particular period of time. Incoming and outgoing bandwidth enforced is 8000000 kbps.
Start Time	Time of the day for the bandwidth rate setting to begin, using a 24-hour clock in local time on the SE (hh:mm).
End Time	Time of the day for the bandwidth rate setting to end, using a 24-hour clock in local time on the SE (hh:mm).

Table 2-25 show bandwidth Field Descriptions (continued)

Field	Description
Default Bandwidth Kbps	Amount of default bandwidth (in kbps). The default bandwidth is the amount of bandwidth associated with each content service type when there is no scheduled bandwidth.
Max Bandwidth Kbps	Maximum bandwidth (in kbps) permitted by the system license. This bandwidth specifies the upper limit of allowable bandwidth.

1. kbps = kilobits per second

Related Commands

Command	Description
bandwidth (Global configuration)	Sets an allowable bandwidth usage limit and its duration for Cisco Streaming Engine WMT streaming media.

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.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-26 describes the fields shown in the **show banner** display.

Table 2-26 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.
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 bitrate

To display the bit rate allocated to a particular device, use the **show bitrate** command in EXEC configuration mode.

show bitrate [**movie-streamer** | **wmt**]

Syntax Description

movie-streamer	(Optional) Displays the Movie Streamer bit rate settings.
wmt	(Optional) Displays Windows Media Technology (WMT) bit rate settings.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-27 describes the fields shown in the **show bitrate** display.

Table 2-27 show bitrate Field Descriptions

Field	Description
Module	Types of application servers for which the bit rate is displayed: • **wmt outgoing** is the maximum bit rate per WMT stream that can be served by the SE. • **wmt incoming** is the maximum bit rate per WMT stream that can be received by the SE. • **movie-streamer outgoing** is the maximum bit rate per streamer that can be served by the SE. • **movie-streamer incoming** is the maximum bit rate per streamer that can be received by the SE.
Default Bitrate Kbps	Bit rate associated with the application servers when the bit rate has not been configured on the SE.
Configured Bitrate Kbps	Bit rate configured on the SE in kilobits per second.

Related Commands

Command	Description
bitrate	Configures the maximum pacing bit rate for large files for the Movie Streamer and separately configures WMT bit-rate settings.

show cache

To display a list of cached contents, use the **show cache** command in EXEC configuration mode.

show cache content *num*

Syntax Description

content	Displays a list of cached contents in order of decreasing priority.
num	(Optional) Number of cached contents to be displayed. The range is from 1 to 1000.

Command Defaults

Number of cached contents is 100.

Command Modes

EXEC configuration mode.

Usage Guidelines

The **show cache** command allows users to check the cached content in an SE.

Use the **show cache content** command to display cache contents, such as priority, size, and URL, and to verify that content has been cached under the correct storage URL. The **show cache content** command also displays the eviction protection information. For relative contents such as WMT and MS, it only displays the parent URL information.

Note When executing the **show cache content** command, the service engine might take sometime if there are prepositioned contents in the **cache**.

Note The **show cache content** command does not display priority (popularity), to see popularity use the **show content-mgr content cache** command or view the Content Manager transaction log entries.

Note When executing the **show cache content url** *url* command on prepositioned content, the output shows as “prepositioned.” However, when executing the **show cache content url** *url* command on hybrid content, it shows as “cached” instead of “prepositioned.” To correct this, use the **detail** option.

Examples

The following example shows how to display the cached contents:

```
ServiceEngine# show cache content 1000
Max-cached-entries is set as 20000000
Number of cal cached assets: 3913
Eviction protection is disabled.
Cache eviction-preferred-size configured is large
-------------------------------------------------
Size         URL
-------------------------------------------------
200000       http://7.6.200.3/B480-Sep18-TEST1/62/file-0-7372
200000       http://7.6.200.3/B480-Sep18-TEST1/62/file-0-6461
```

```
200000       http://7.6.200.3/B480-Sep18-TEST1/99/file-0-9701
200000       http://7.6.200.3/B480-Sep18-TEST1/99/file-0-4429
200000       http://7.6.200.3/B480-Sep18-TEST1/99/file-0-8867
200000       http://7.6.200.3/B480-Sep18-TEST1/67/file-0-3360
200000       http://7.6.200.3/B480-Sep18-TEST1/927/file-0-4481
200000       http://7.6.200.3/B480-Sep18-TEST1/927/file-0-5002
200000       http://7.6.200.3/B480-Sep18-TEST1/44/file-0-4454
200000       http://7.6.200.3/B480-Sep18-TEST1/105/file-0-4643
200000       http://7.6.200.3/B480-Sep18-TEST1/291/file-0-544
<Output truncated>
```

Related Commands

Command	Description
cache	Configures the cached content maximum entries in the CDS.

show cache-router

To Display cache-router information for various Protocol Engines, use the **show cache-route** command in EXEC configuration mode.

show cache-router {**routes** {**dss-engine** *url* | **fms-engine** *url* | **web-engine** *url* | **wmt-engine** *url* | **upstream-status**}

Syntax Description

routes	Displays the cache-route information for various PEs.
dss-engine	Displays all RTSP protocol-related cache route information.
url	URL string.
fms-engine	Displays all Flash Media-related cache route information.
web-engine	Displays all HTTP protocol-related cache route information.
wmt-engine	Displays all Windows Media-related cache route information.
upstream-status	Displays Liveness information of upstream.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

This command can only be run on an SE to see the route taken by the appropriate Protocol Engine through the CDN (from the current SE where this command is executed) to retrieve the asset for a given URL.

The **sh cache-router routes** command route calculation is agnostic of whether or not the URL is valid.

When a new SE is added to a delivery service, the get_cache_route does not vie the path, the command dumps the cached output and does not perform a liveness query. You must first enter the **show cache router upstream status** command and then the commands in the following example:

Examples

The following examples show the cache route information:

```
ServiceEngine# sh cache-router routes web-engine http://7.25.0.7/index.html
The route: [ 7.25.0.15/7.25.0.13/ ] will be used to cache the asset for
URL=http://7.25.0.7/index.html

ServiceEngine# sh cache-router routes web-engine http://7.25.0.7/index.html
The route: [ 7.25.0.13/ ] will be used to cache the asset for
URL=http://7.25.0.7/index.html

ServiceEngine# sh cache-router routes web-engine http://7.25.0.7/index.html
The route: [ (null) ] will be used to cache the asset for URL=http://7.25.0.7/index.html

ServiceEngine# sh cache-router routes web-engine
               http://ccp-ccp-images.gslb.bdn.lab.xcal.tv/image1
The route: [ 69.241.50.154/69.252.83.150/69.241.118.14/ ] will be used to cache the asset
for URL=http://ccp-ccp-images.gslb.bdn.lab.xcal.tv/image1.
```

show capability

To display the capabilities of the Cap-X profile ID, use the **show capability** command in EXEC configuration mode.

show capability profile ID *profile_id*

Syntax Description

profile ID	Displays information for the Cap-X profile.
profile_id	Profile ID number. The range is from 1 to 65535.

Command Defaults

None

Command Modes

EXEC configuration mode.

Related Commands

Command	Description
capability	Modifies the capability configuration.

show cdn-select

To display the status of the CDN Selector, use the **show cdn-select** command in EXEC configuration mode.

show cdn-select

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Related Commands

Command	Description
cdn-select	Enables the CDN Selector for third-party service selection.
geo-location-server	Redirects requests to different CDNs based on the geographic location of the client.
show statistics cdn-select	Displays the statistics for the CDN Selector.

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 CDSNFS volumes.

Command 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 2-28 describes the fields shown in the **show cdnfs volumes** display.

Table 2-28 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 2-29 describes the fields shown in the **show cdnfs usage** display.

Table 2-29 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 cachable.

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 Internet Streamer CDS network file system (cdnfs).
disk (EXEC)	Configures disks and allocates disk space for devices that are using the CDS 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.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The CDS 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 2-30 describes the field in the **show clock** display.

Table 2-30 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 UTC offset.

Table 2-31 describes the fields shown in the **show clock detail** display.

Table 2-31 show clock detail Field Descriptions

Field	Description
Local time	Local time relative to UTC.
UTC time	Coordinated Universal 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 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.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-32 describes the fields shown in the CDSM **show cms info** display.

Table 2-32 show cms Field Descriptions for the CDSM

Field	Description
CDN information	
Model	Model name of the device.
Node Id	Unique identifier given to the device by the CDSM at registration, which is used to manage the device.
Device Mode	Configured mode of device used during registration.
Current CDSM role	Role of the current CDSM: 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 CDSM only.
Service cms_cdsm is running	Status of the cms_cdsm management service (running or not running). This field is specific to the CDSM only.

Table 2-33 describes the fields shown in the SE **show cms info** display.

Table 2-33 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 CDSM at registration, which is used to manage the device.
Device Mode	Configured mode of device used during registration.
Current CDSM address	Address of the CDSM as currently configured in the **cdsm ip** command in Global configuration mode. This address may differ from the registered address if a standby CDSM is managing the device instead of the primary CDSM with which the device is registered.
Registered with CDSM	Address of the CDSM with which the device is registered.
Status	Connection status of the device to the CDSM. 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 CDSM for updates.

The following example writes the database content to a file in text format:

```
CDSM# 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:

```
CDSM# 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 CDS, 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.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

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.

Note For the value of the symlink output field to be correct for the Flash Media Streaming engine, you must configure the play server as HTTP by using the Manifest file.

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, 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 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.cds.com/vod/pinball.wmv
        Status is 3 (Servable)
        Content is Complete
        File size is 0 Bytes
        Playable by WebEngine WMT
        Linked to
[rtsp://http-we-os.cds.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.cds.com/1d/a1/1da1394af838bbcb45af78fd5681abeb/pinball.w
mv]

Protocol Engine Metadata:
        Authorization is Not Required
        uns_attr_symlink :
http-we-os.cds.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 RTSP URL in the CDS:

```
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
Playable by WMT
Authorization is Not Required
Content is CACHED with priority 0.574964
```

The following example shows how to display all content entries in the CDS:

```
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
        Playable by WMT
        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 WebEngine
        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 WebEngine
        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 WebEngine
        Content is CACHED
```

show content-mgr

To display all content management information in the CDS, use the **show content-mgr** command in EXEC configuration mode.

show content-mgr {**content** {**all** {**all-disk-volumes output-file** *filename* | **disk-volume output-file** *filename*| **cache** {**all-disk-volumes output-file** *filename* | **disk-volume output-file** *filename* | **prepos** {**all-disk-volumes output-file** *filename* | **disk-volume output-file** *filename}* | **disk-info** | **eviction-list size** *num* {**all-disk-volumes output-file** *filename* | **disk-volume output-file** *filename* | **eviction-protection output-file** *filename* | **health-info**}

Syntax Description

content	Dumps Content Manager objects with priority, url, or disk path.
all	Dumps cached and prepositioned contents.
all-disk-volumes	Dumps all disks.
output-file	Specifies the output filename to write to.
filename	The output file name to write to.
cache	Dump cached contents.
disk-volume	Specifies the disks to be dumped.
prepos	Dump prepositioned contents.
disk-info	Displays disk information.
eviction-list	Dumps the list of contents which is evicted first.
size	Specifies the eviction size (in MB).
eviction-protection	Dumps eviction protection table.
health-info	Displays health information.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **show content-mgr content all** command dumps all the contents to the specified output file. This process goes through the entire Content Manager data structure to collect file information, and then writes it into the file specified by the user. When the Content Manager begins to dump the records, it states the number of records it prepares to write and how many are actually written in the ~/errorlog/content_manager.current file.

The following example shows a dump with no object being deleted:

```
03/18/2011 23:32:34.945(Local)(9633)LOG :ContentMgr.cpp:968-> Scheduled prepositioned
entries[1] for dump
03/18/2011 23:32:34.945(Local)(9633)LOG :CMgrDumpStore.cpp:75-> Starting dump, entries[1]
03/18/2011 23:32:34.946(Local)(9633)LOG :CMgrDumpStore.cpp:97-> Dump finished.
```

The following example shows a dump with objects being deleted:

```
14:03/18/2011 23:36:20.195(Local)(9633)LOG :ContentMgr.cpp:951-> Scheduled cached
entries[81931] for dump
```

```
14:03/18/2011 23:36:20.195(Local)(9633)LOG :CMgrDumpStore.cpp:75-> Starting dump,
entries[81931]
14:03/18/2011 23:36:23.764(Local)(9633)LOG :CMgrDumpStore.cpp:97-> Dump finished. Entries
removed during dump[41931]. These will not show up in the output file.
```

The **show content-mgr disk-info** command prints disk and asset information for the Content Manager monitors.

Examples

The following example shows how to display all the Content Manager disk information in an output file:

```
ServiceEngine# show content-mgr content all all-disk-volumes output-file dumps
#type-tail dumps
#ContentType Priority URL DiskPath
cached-content 6 http://5.3.3.10/a_1/file_10005542
/disk00-06/c/5.3.3.10/5f/37/5f37c0748805ddf6e58a63853b3677af/file_10005542.http
prepos-content 0 http://172.22.67.108/vod/FootballHD.flv
/disk08-01/p/172.22.67.108/1d/a1/1da1394af838bbcb45af78fd5681abeb/FootballHD.flv
prepos-content 0
://172.22.67.108/manifest-Channel_5683.xml-FNtiIA2L9GVRqiFKzK-h3w
/disk04-01/p/172.22.67.108/66/66/6666cd76f96956469e7be39d750cc7d9/_7279f4d
49c9963f509d8ad2cd772fdf6
prepos-content 0
://http-172.22.67.108-89xld465l9xq3fuq2dgi5w/vod/abc.html
/disk06-01/p/http-172.22.67.108-89xld465l9xq3fuq2dgi5w/1d/a1/1da1394af838bbcb45af7
8fd5681abeb/abc.html
```

The following example shows how to display the Content Manager disk information:

```
ServiceEngine# show content-mgr disk-info
Mount point : /disk00-01
     Bucket Number Assigned to Disk : 0
     File system                    : CDNFS
     Total space                    : 423.6 GB
     Free space                     : 415.1 GB
     Disk Eviction low watermark    : 381.3 GB
     Disk Eviction high watermark   : 394.0 GB
     Writable                       : Yes
     Usable                         : Yes
     Preposition Asset Count        : 0
     Cache Asset Count              : 0
     Preposition Asset Size         : 0 B
     Cache Asset Size               : 0 B
```

The following example shows how to display the Content Manager health information:

```
ServiceEngine# show content-mgr health-info

Deletion Task Count           : 0
Deletion Store Size
     disk00-06                : 0 B
     disk01-06                : 0 B
     disk02-01                : 0 B
Protection Table Size         : 0 B
Snapshot In Progress          : No
Eviction In Progress          : No
Slow scan In Progress         : No
Sanity In Progress            : No
Clear Cache All In Progress   : No
Dump In Progress              : No
Priority Queue Asset Count    : 0
HitCount Decay Half Life (days): 14
Disk Bucket Alarm Threshold(%): 30
```

```
------------------------   Printing All Asset Info   ------------------------

Mount Point                    : disk00-06
Preposition Asset Count        : 4
Cache Asset Count              : 0
Preposition Asset Size         : 104 B
Cache Asset Size               : 0 B

Mount Point                    : disk01-06
Preposition Asset Count        : 8
Cache Asset Count              : 0
Preposition Asset Size         : 312 B
Cache Asset Size               : 0 B

Mount Point                    : disk02-01
Preposition Asset Count        : 2
Cache Asset Count              : 0
Preposition Asset Size         : 52 B
Cache Asset Size               : 0 B

Memory pool statistics   : [      Used][      Free][  Max Used]
Cached File Nodes        : [         0][         0][         0]
Cached Child Nodes       : [         0][         0][         0]
Cached Dir Nodes         : [         1][       818][         1]
Prepos File Nodes        : [        14][    220738][        15]
Prepos Child Nodes       : [        48][    262096][        49]
Prepos Dir Nodes         : [        35][       784][        35]

------------------------   Printing Process Status  ------------------------
CPU Usage Percent              : 0.00
Threads Count                  : 33
Virtual Memory Size            : 189.6 MB
Resident Memory Size           : 33.4 MB

------------------------ Printing Delivery Services ------------------------

Delivery Service Id            : 1450
Origin FQDN                    : 172.22.67.227
Routing Domain Name            : vodplay1.com

Delivery Service Id            : 1272
Origin FQDN                    : 1.2.3.5
Routing Domain Name            : livewmtplay.com

Delivery Service Id            : 1262
Origin FQDN                    : 171.71.51.234
Routing Domain Name            : wmtplay.com

Delivery Service Id            : 1260
Origin FQDN                    : 172.22.67.108
Routing Domain Name            : vodplay.com
```

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 statistics content-mgr	Displays the Content Manager statistics.

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 FQDN.
domain	Domain of the request FQDN.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

Table 2-33 describes the fields shown in the **show content-origin** display.

Table 2-34 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:

```
Cds Origin Manager writes syslog messages when NAS mount fails. Below are some sample
syslog messages:
Apr 28 04:25:26 nas-se CdsOriginMgr: %SE-CdsOriginMgr-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/WMT
```

```
      MountPoint: WMT
      Status: Failed
      MaxRetry: 10
      RetryCount: 17

      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 servers 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 [ip {bgp | ospf | proximity | rib} | isis | srp | svc {desci | registry}]

Syntax Description

ip	(Optional) Displays the debug options for IP.
bgp	Displays the debugging flags that have been set for BGP.
ospf	Displays the debug options for OSPF processes that are enabled.
proximity	Displays the debug options that are enabled for the proximity process.
rib	Displays the debug options that are enabled for the rib process.
isis	(Optional) Displays the debug options that are enabled for the IS-IS process.
srp	(Optional) This command displays the debug flags that are turned on for the SRP.
svc	(Optional)
desci	Descriptor Interpreter Library.
registry	Service Registration Daemon.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

The **show debugging ip bgp** command is used to display the debugging flags that have been set for BGP.

The **show debugging ip ospf** command is used to display debug options for OSPF processes that are enabled.

The **show debugging ip rib** command is used to display debug options for rib processes that are enabled.

The **show debugging isis** command is used to display debug options for IS-IS processes that are enabled.

The **show debugging srp** command is used to displays the debug flags that are turned on for the SRP.

Examples

The following is sample output from the **show debugging ip bgp** command:

```
ServiceRouter# debug ip bgp keepalives
ServiceRouter# show debugging ip bgp
BGP keepalives debug is on
ServiceRouter# debug ip bgp all
ServiceRouter# show debugging ip bgp
BGP events debug is on
BGP internal debug is on
BGP RIB debug is on
BGP BRIB debug is on
BGP updates debug is on
```

```
BGP keepalives debug is on
BGP packets debug is on
BGP IO debug is on
BGP list debug is on
BGP dampening debug is on

ServiceRouter#
```

The following is sample output from the **show debugging ip ospf** command:

```
ServiceRouter# show debugging ip ospf

All OSPF debug is on
Adjacency events debug is on
OSPF LSDB changes debug is on
OSPF LSDB timers debug is on
OSPF related events debug is on
LSA flooding debug is on

ServiceRouter#
```

The following is sample output from the **show debugging isis** command.

```
ServiceRouter# show debugging isis

SRP error debug is on
SRP api debug is on
SRP multicast debug is on
SRP session debug is on
SRP srhp packet debug is on
SRP replica debug is on
SRP packet asiii debug is on
SRP function debug is on
SRP replay is on

ServiceRouter#
```

The following example shows the use of **show srp debug** command:

```
ServiceRouter# show debugging srp

SRP packet debug is on
SRP error debug is on
SRP database debug is on
SRP api debug is on
SRP host debug is on
SRP multicast packet debug is on
SRP session debug is on
SRP srhp packet debug is on
SRP replica debug is on
SRP sync debug is on
SRP configuration debug is on
SRP ippc debug is on
SRP packet ascii debug is on
SRP function debug is on

ServiceRouter#
```

In the following example, the **debug icp client** command coupled with the **show debugging** command shows that Internet Cache Protocol (ICP) debugging is enabled:

```
ServiceEngine# debug icp client
ServiceEngine# show debugging
Debug icp (client) is on
```

Related Commands

Command	Description
debug	Monitors and records caching application functions.
undebug	Disables debugging functions.

show debugging srp

To display the debug flags that are turned on for SRP, use the **show debugging srp** command in privileged EXEC mode.

show debugging srp

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC configuration mode.

Examples

The following example shows the use of **show debugging srp**:

```
ServiceRouter# show debugging srp

SRP packet debug is on
SRP error debug is on
SRP database debug is on
SRP api debug is on
SRP host debug is on
SRP multicast packet debug is on
SRP session debug is on
SRP srhp packet debug is on
SRP replica debug is on
SRP sync debug is on
SRP configuration debug is on
SRP ippc debug is on
SRP packet ascii debug is on
SRP function debug is on

ServiceRouter#
```

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.

Command 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 CDS 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 CDSM, SE or SR.

show direct-server-return

To display the Direct Server return information, use the **show direct-server-return** command in EXEC configuration mode.

show direct-server-return

Syntax Description

This command has no keywords or arguments.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to display the Direct Server return information:

```
ServiceEngine# show direct-server-return
direct-server-return vip 11.11.11.11
```

Related Commands

Command	Description
direct-server-return	Enables a VIP for direct server return.

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 SMART disk monitoring info with more details.

Command 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 2-35 describes the fields shown in the **show disks details** display.

Table 2-35 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 2-36 describes the fields shown in the **show disks error-handling details** display.

I/O e

Table 2-36 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 CDS 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 CDS software monitors the SMART attributes and reports any impending failure through syslog messages, SNMP traps, and alarms.

The output from the **show tech-support** command in EXEC configuration mode also includes SMART information.

Table 2-37 describes some typical fields in the **show disks SMART-info** display.

Table 2-37 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 2-37 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 CDS software.

show distribution

To display the distribution information for a specified delivery service and to probe a remote SE for the liveness of its associated delivery service, use the **show distribution** command in EXEC configuration mode.

show distribution [**delivery-services** {**delivery-service-id** *delivery_service_num* | **delivery-service-name** *delivery_service_name*} | **forwarder-list** {**delivery-service-id** *delivery_service_num* | **delivery-service-name** *delivery_service_name*} | **detail** | **location** {**forwarder-load-weight** | **live-load-weight** | **location-leader-preference**} {**delivery-service-id** *delivery_service_num* | **delivery-service-name** *delivery_service_name*} | **mcast-data-receiver** {**channels** | **cloud detail**} | **mcast-data-sender** {**channels** | **cloud detail**} | **object-status** *object_url* | **processes** | **remote** *ip_address* {**metadata-sender** {**delivery-service-id** *delivery_service_num* [**start-generation-id** *gen_id* **end-generation-id** *gen_id*] | {**delivery-service-name** *delivery_service_name* [**start-generation-id** *gen_id* **end-generation-id** *gen_id*]} | **unicast-sender** {**delivery-service-id** *delivery_service_num* {**cdn-url** *cdn_url* | **probe** | **relative-cdn-url** *cdn_url*}} | **delivery-service-name** *delivery_service_name* {**cdn-url** *cdn_url* | **probe** | **relative-cdn-url** *cdn_url*}} | **traceroute** {**forwarder-next-hop delivery-service-id** *delivery_service_num* {**max-hop** *maxhop_num* | **trace-till-good** | **trace-till-root**}} | **unicast-sender delivery-service-id** *delivery_service_num* {**cdn-url** *cdn_url* | **probe** | **relative-cdn-url** *cdn_url*} {**max-hop** *maxhop_num* | **trace-till-good** | **trace-till-root**}}]

Syntax Description

delivery-services	(Optional) Displays information about the specified delivery service.
delivery-service-id	(Optional) Specifies the delivery service ID.
delivery_service_num	Delivery service number (64-bit number).
delivery-service-name	(Optional) Specifies the delivery service name.
delivery_service_name	Delivery service name.
forwarder-list	(Optional) Displays the forwarder lists for all delivery services subscribed to by the SE.
detail	(Optional) Displays detailed forwarder lists for all delivery services subscribed to by the SE.
location	(Optional) Displays delivery service routing-related parameters for the SEs in the location (specified by the delivery service ID).
forwarder-load-weight	Displays the forwarder load weight value of the SEs in the location (specified by the delivery service ID). For more information, see the "Forwarder Probability" section on page 2-390.
live-load-weight	Displays the live load weight value of the SEs in the location (specified by the delivery service ID). For more information, see the "Live Splitting Probability" section on page 2-392.
location-leader-preference	Displays the location leader preference value of the SEs in the location (specified by the delivery service ID). For more information, see the "Location Leader Preference" section on page 2-391.
mcast-data-receiver	Display Multicast Data Receiver information.
channels	(Optional) Displays the list of channels assigned.
cloud	(Optional) Displays the cloud configuration.
detail	(Optional) Displays detailed cloud configuration.

mcast-data-sender	Displays Multicast Data Sender information.
object-status	(Optional) Displays information on the status of a prepositioned object.
object_url	URL of the prepositioned object.
processes	(Optional) Displays information on distribution processes.
remote	(Optional) Displays delivery service information about a remote SE.
ip_address	IP address of the remote SE.
metadata-sender	Displays the metadata from a remote SE.
start-generation-id	(Optional) Specifies the beginning database value of the current version of the multicast cloud.
gen_id	Beginning database value.
end-generation-id	Specifies the ending database value of the current version of the multicast cloud.
gen_id	Ending database value.
unicast-sender	Displays the unicast data from a remote SE.
cdn-url	Checks the object on a remote SE using the specified URL.
cdn_url	CDS network URL used to check the object on a remote SE.
probe	Probes the remote unicast sender.
relative-cdn-url	Checks the object on a remote SE using the specified URL.
traceroute	Displays the traceroute for the delivery service routing status.
forwarder-next-hop	Displays the next forwarder in the path for the SE. **Note** This keyword lets you display the forwarding SEs to the Content Acquirer in a manner similar to the **traceroute** command.
delivery-service-id	Specifies the delivery service ID with which the unicast sender is associated.
delivery_service_num	Delivery service number of the delivery service with which the unicast sender is associated.
max-hop	Displays the maximum number of hops needed to reach the unicast sender.
maxhop_num	Maximum number of hops. The range is from 1 to 1024.
trace-till-good	Allows the device to trace the route of an object until the object is found.
trace-till-root	Allows the device to trace the route of an object until the device reaches the Content Acquirer.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use the **show distribution remote** *ip_address* **metadata-sender delivery-service-id** *delivery_service_num* [**start-generation-id** *gen_id* **end-generation-id** *gen_id*] command option to retrieve the metadata from a remote SE assigned to a specified delivery service ID. The start and end generation IDs specify the beginning and ending database values representing the current version of the multicast cloud stored in the local database.

Note Generation IDs must be greater than zero. Also, you must specify both the start and the end generation IDs, or neither ID.

The **show distribution remote** *ip_address* **unicast-sender delivery-service-id** *delivery_service_num* **relative-cdn-url** *cdn_url* command shows the status of the relative CDS network URL of an object at a remote SE assigned to a specified delivery service ID. A relative CDS network URL is one that lacks the prefix of the protocol and hostname. For example, the relative CDS network URL for http://www.mycompany.com/abc.def.html is abc.def.html.

Use the **show distribution remote** *ip_address* **unicast-sender delivery-service-id** *delivery_service_num* **probe** command to probe a remote SE for the liveness of the delivery service to which it is assigned.

The **show distribution object-status** *object_url* command can be used to display the properties of a prepositioned object.

You can view the location leader preference and forwarder weight for the SE using the **show distribution** command. However, you can configure the location leader preference and forwarder weight only using the CDSM GUI for each SE. Default values are assumed if you do not manually configure them.

The **show distribution location forwarder-load-weight** command displays the probability of SEs assigned to the delivery service within the location being selected as a forwarder. The **show distribution location location-leader-preference** command displays the location leader preference value of SEs that are assigned to the delivery service within the location.

Use the **show distribution delivery-services** command to view the forwarder for the SEs. If a receiver SE is unable to find its forwarder SE, one of the following reasons is displayed in the Status/Reason column of the output of the **show distribution delivery-services** command:

- LLMT—Home SE cannot find the forwarder because the home SE has a limit on the forwarder lookup level.
- FAIL—Home SE cannot find the forwarder because there is a failed SE along the path within the specified forwarder lookup level.
- NGWT—Home SE cannot find the forwarder because there is an SE with a negative forwarder-load-weight along the path within the specified forwarder lookup level.

Use the **show distribution mcast-data-sender** and **show distribution mcast-data-receiver** commands to see a list of assigned channels and cloud configuration for the Multicast data senders and receivers that were added to the Multicast cloud using the **multicast** command.

Forwarder Probability

When an SE (location leader) selects its forwarder from an upstream location, it uses the *forwarderLoad_weight* value configured for each SE in its upstream location. The weight value of each SE corresponds to the probability of the SE being selected as the forwarder.

Each SE generates a unique random number. When an SE needs to select an inter-location forwarder, it views all the SEs in one remote location as a collection, with the size corresponding to their weight. It uses the generated random number to select an SE as a forwarder. SEs with a higher weight are more likely to be selected as forwarders.

Note The *forwarderLoad_weight* value represents a probabilistic value. When a large number of children SEs select a forwarder from a location, the load on the forwarder represents the weight.

The load on the forwarder is the replication load per delivery service on the SE because all SEs subscribed to the delivery service select a forwarder to balance the load. However, as the number of SEs assigned to different delivery services might differ, a forwarder might receive requests for content from SEs in other delivery services, which increases the load. Therefore, it is possible that the total load (of replicating content) on the forwarder does not reflect the weight but depends on the number of SEs assigned to a delivery service.

For each SE, you can specify the probability of each SE acting as a forwarder to SEs from downstream locations using the CDSM GUI. You can also specify whether certain SEs should never serve as a forwarder to downstream SEs. The specification is delivery service independent.

If you choose not to configure settings using the Location Leader and Forwarder Settings for SE window, the delivery service routing algorithm uses the random number method to generate one permutation of the SE ID ordered list.

Location Leader Preference

For intra-location (list of SEs in an SE's own location) forwarder selection, the delivery service routing algorithm first creates an ordered list of the SEs based on their *location leader preference* in a descending order. Next, the delivery service routing algorithm selects the first SE in the ordered list as the location leader.

When multiple SEs have the same *location leader_preference*, the delivery service routing algorithm guarantees that all the SEs assigned to each delivery service in the location still generate the same ordered list, which avoids routing loops. A routing loop is a deadlock situation in which the forwarder selection among multiple SEs within the loop prevents the SEs from receiving the content from upstream locations. For example, SE1 uses SE2 as the forwarder and SE2 uses SE1 as the forwarder for the same delivery service.

However, for two different delivery services, the ordered list could be different (when multiple SEs have the same location leader probability value) even if the subscribed SEs are the same. When multiple SEs have the highest *location leader_preference*, although each SE has an equal chance of acting as the location leader (for different delivery services), only one SE always acts as the location leader for one particular delivery service. If you configure all the SEs in your network to have the same *location leader_preference* value, then each SE has an equal chance of acting as a location leader. When each SE has an equal probability of being selected as the location leader for any particular delivery service, only one particular SE is always selected as the location leader.

Note If there are two SEs in the same location (SE1, SE2) and both of them are assigned to two delivery services (CH1, CH2), and if you want SE1 to be the location leader for CH1 and SE2 to be the location leader for CH2, you cannot configure them using *location leader_preference* and *forwarderLoad_weight*.

In a location, you can specify the probability for each SE acting as the location leader. The specification is delivery service independent.

The following limitations are associated with specifying a location leader preference:

- When multiple SEs are configured with the same *location leader_preference* value and assigned to a delivery service, they have an equal probability of being selected as the location leader. In such a case, you do not have a control mechanism to decide which SE should be selected as the location leader.

- Only the order among the SEs with the highest preference is randomized to determine the location leader preference and not other SEs with the same preference value. It is possible that if the SE(s) with the highest preference failed and there are several other SEs with the second highest preference value, they are not balanced across the different delivery services. The same SE is the location leader for all delivery services.
- If an SE with a high *location leader_preference* is assigned to many delivery services, it is possible that the SE can be selected as the location leader for all these delivery services.

Live Splitting Probability

Similar to the delivery service routing application used for content replication that assigns weight and priority to SEs to tune location leader and forwarder selections, you can specify a configuration parameter *liveSplit_load_weight* for each SE. This parameter represents the relative probability that an SE is likely to receive live stream splitting traffic as compared to other SEs. The specification is delivery service independent. If you do not configure *liveSplit_load_weight*, the algorithm should work as it currently does.

A weighted load balancing scheme splits the live stream load on the SEs according to the *liveSplit_load_weight* value because SEs of different types have an equal probability of being selected as the splitting SE on the location path.

The *liveSplit_load_weight* is used when the delivery service routing generates the ordered list of SEs for each location. The SEs are ordered in a way that the higher the weight, the greater probability that the SEs are being ordered at the beginning of the list.

The weight represents a relative value. The *liveSplit_load_weight* assigned to one SE is compared against the weights of other SEs in the same location.

The weight is a probabilistic value. For one particular URL, all SEs generate the same ordered list for a location.

It is possible that an SE with a lower weight is being ordered at the beginning while an SE with a higher weight is being ordered at the end of the list. The weighted load balancing is useful only when there are multiple live stream URLs.

The *liveSplit_load_weight* parameter applies both within the home location and upstream locations. This setting is different from the distribution settings where locationLeader-priority controls how you choose SEs from the home location, while forwarderLoad-weight controls how you choose SEs from upstream locations.

Examples

The following example shows the status of the object at a remote SE with the IP address 172.16.2.160 and delivery service ID 631. The URL of the content object specified in the command must not be the complete source URL. Instead, it must be the relative CDS network URL of the object.

```
ServiceEngine# show distribution remote 172.16.2.160 unicast-sender delivery-service-id
631 relative-cdn-url 101files/100.txt

     Forwarder-Name :                AD-SE08
       Forwarder-ID :                   140
       Forwarder IP :            2.43.10.70
 Forwarder Location :       default-location
Relative CDN URL :       101files/100.txt
        Actual Size :                    58
   Size Transferred :                    58
        Resource-ID : roVe2aMzp+YhmbhGUfMPpQ
         Content-ID : 7LC5xOlMp4YvkBJlHaQucQ
Last Modified Time :   10:52:38 Jan 04 2005
```

The following example retrieves the metadata from a remote SE with the IP address 172.16.2.160 assigned to delivery service ID 4999:

```
ServiceEngine# show distribution remote 172.16.2.160 metadata-sender delivery-service-id
4999

Getting meta data for delivery service(4999) from genid -1 to 2
Connecting to 2.43.10.101
Remote SE replied with the following headers:
        Action : Processing metadata records
        Latest Gen id is : 2
        Have more records to process : No
        Is metadata still in full reload: No
add-size: 2, del-size: 0

Add Logs: 1 to 2
        add # 1: UBsSUMwbTdJzzpqDvxSdYg.., basic_auth/public.html
        add # 2: NJyVL9CZwpnyCfw+Is26yw.., index.txt
```

The following example probes the remote SE with the IP address 172.16.2.160 for the liveness of its assigned delivery service ID 153:

```
ServiceEngine# show distribution remote 172.16.2.160 unicast-sender delivery-service-id
153 probe
Probe Successful
```

The following example shows the beginning database value of the current version of the multicast cloud at a remote SE with the IP address 10.43.10.101 and delivery service ID 4999:

```
ServiceEngine# show distribution remote 10.43.10.101 metadata-sender delivery-service-id
4999 start-generation-id 0 end-generation-id 5
Getting meta data for delivery service(4999) from genid -1 to 5
Connecting to 10.43.10.101
Remote SE replied with the following headers:
        Action : Processing metadata records
        Latest Gen id is : 2
        Have more records to process : No
        Is metadata still in full reload: No
add-size: 2, del-size: 0

Add Logs: 1 to 2
        add # 1: UBsSUMwbTdJzzpqDvxSdYg.., basic_auth/public.html
        add # 2: NJyVL9CZwpnyCfw+Is26yw.., index.txt
```

Note When start and end generation IDs are not specified in the **show distribution remote** command, the current maximum generation ID of –100 is the start generation ID. The end generation ID is equal to the sum of the start generation ID and 100.

The following example shows the list of forwarders in the path toward the Content Acquirer:

```
ServiceEngine# show distribution remote traceroute forwarder-next-hop delivery-service-id
4999 trace-till-root

Hop NextHop_SEId  NextHop_SEName NextHop_SEIp      GenID Status/Reason
--- ------------  -------------- ------------      ----- -------------
  1    5884            AD-SE07    192.168.1.69     1        REGULAR
  2    6035            AD-SE13     2.43.10.101     1       LOC-LEAD
  3    5683            AD-SE12     2.43.10.100     1       LOC-LEAD
  4    6026       gnadaraj-507       2.43.27.2     1       LOC-LEAD
  5    5638           devi-507      2.43.27.36     1       LOC-LEAD (Reached RootSE)
```

The following example shows output from the **show distribution object-status** command:

```
ServiceEngine# show distribution object-status http://www.cisco.com/index.txt

        ========== Website Information ==========

Name                       :          cisco-crawl
Origin Server FQDN         :        www.cisco.com
Request Routed FQDN        :                 N/A
Content UNS Reference #    :                   1

        ========== delivery services Information ==========

        *** delivery service 4999 (name = headercheck) ***

Object Replication
------------------
Replication                :                      Done
File State                 :    Ready for distribution
Multicast for delivery service     :               Not Enabled
Replication Lock           : Received by Unicast-Receiver/Acquirer
Reference Count            :                         1
Total Size                 :                   2208640
Transfered Size            :                   2208640
MD5 of MD5                 :  zwhJagyCmRAE4UmTwc0EtA..
Source Url                 : http://liqq-linux.cisco.com/index.txt
Source Last Modified Time  :  Sun Jul 11 03:23:33 2004

Object Properties
-----------------
Redirect To Origin         :                      Yes
Requires Authentation      :                       No
Alternative URL            :
Serve Start Time           :                      N/A
Serve End Time             :                      N/A
Play servers               :                HTTP HTTPS
Content Metadata           :                     None
Content uns_id             :  yhzR3VZ96MDz5FVHwmGD+A..
Content gen-id             :         5638:1108022220:1

        ========== CDNFS Information ==========

Internal File Name         :
/disk00-04/d/http-liqq-linux.cisco.com-azk2lrqzsytweswexham5w/32/326cf0278da48aac82d796cb1
19b1caa.0.data.txt
Actual File Size           : 2208640 bytes
MD5 of MD5 (Re-calculated): zwhJagyCmRAE4UmTwc0EtA..
Content metadata           : None
Metadata match with        : delivery service 4999
Number of Source-urls      : 1

        Source-url to CDN-object mapping:

        Source-url                : http://liqq-linux.cisco.com/index.txt
        Used by CDN object        : ---- Yes ----
        Internal File Name        :
/disk00-04/d/http-liqq-linux.cisco.com-azk2lrqzsytweswexham5w/32/326cf0278da48aac82d796cb1
19b1caa.0.data.txt
        Actual File Size          : 2208640 bytes

        ========== CDNFS lookup output ==========

CDNFS File Attributes:
  Status                3  (Ready)
  File Size             2208640 Bytes
  Start Time            null
```

```
  End Time               null
  Allowed Playback via   HTTP HTTPS
  Last-modified Time     Sun Jul 11 03:23:33 2004
  cdn_uns_id             yhzR3VZ96MDz5FVHwmGD+A..
  last-modified          Sun, 11 Jul 2004 03:23:33 GMT
Internal path to data file:
/disk00-04/d/http-liqq-linux.cisco.com-azk2lrqzsytweswexham5w/32/326cf0278da48aac82d796cb1
19b1caa.0.data.txt
```

The **show distribution delivery-services** output and the **show distribution forwarder-list** output display additional delivery service routing information. The newly added Status/Reason field displays whether the SE is a location leader and the reason for not having a forwarder SE.

The following example shows the delivery service distribution information:

```
ServiceEngine# show distribution delivery-services
Delivery Service Name   ID   Priority   Root Forwarder   Status/Reason
------------   --   --------   ---- ---------   -------------   ----------
00-AD          527      500    No    Rack89-SE-11   REGULAR         N/A
01-AD          586      500    Yes   N/A            N/A             N/A
00-Live        588      500    Yes   N/A            LIVE            N/A

  LOC-LEAD:   This SE is the location leader for this delivery service
   REGULAR:   This SE is not the location leader for this delivery service
      LLMT:   This SE cannot find forwarder because this SE has limit on
              the forwarder lookup level
      FAIL:   This SE cannot find forwarder because there is failed SE along
              the path within specified forwarder lookup level
      NGWT:   This SE cannot find forwarder because there is SE with negative
              forwarder-load-weight along the path within the specified
              forwarder lookup level
      LIVE:   The specified delivery service is live delivery service, forwarder not
applicable
         *:   MetaData forwarder and Unicast forwarder are different
```

The following example provides delivery service distribution information for delivery service ID 527:

```
ServiceEngine# show distribution delivery-services delivery-service-id 527
Delivery service Configuration
----------------------
Delivery service ID                          :                 527
Delivery service Name                        :               00-AD
Website Name                        :               Test1
Website Origin FQDN                 :         www.test.com
Delivery service Priority                    :                 500
Configured Distribution Type        :       Multicast only

Content Acquirer Information
--------------------
ID of Configured Content Acquirer            :                 462
Name of Configured Content Acquirer          :         Rack89-SE-11
IP of Configured Content Acquirer            :           2.43.27.38
ID of Effective Content Acquirer             :                 462
Current root-ce-uid                 :           1110247321
This SE's Role                      :       Not a Content Acquirer
This SE in Full Reload              :                  No

Content Acquirer Failover/Fallback Information
---------------------------------------
Content Acquirer Failover/Fallback Interval :             120 Mins

Metadata Information
--------------------
Metadata-Forwarder ID               :                 462
```

```
Metadata-Forwarder Name             :          Rack89-SE-11
Metadata-Forwarder Primary IP       :            2.43.27.38
Metadata-Forwarder NAT IP/Port      :                   N/A
Address to Poll Metadata-Forwarder  :            Primary IP
Metadata-Forwarder Status           :               REGULAR
Last gen-id Switch                  :                 Never
Current low-water-marker            :                     1
Current max-gen-id                  :                     0
Current max-del-gen-id              :                     0
Last poll                           :           13 Secs ago
Next poll                           :     107 Secs from now
Idle poll interval                  :              120 Secs
Poll interval multiplier            :                     1

Unicast Information
-------------------
Ucast-Forwarder ID                  :                   462
Ucast-Forwarder Name                :          Rack89-SE-11
Ucast-Forwarder Primary IP          :            2.43.27.38
Ucast-Forwarder NAT IP/Port         :                   N/A
Address to Poll Ucast-Forwarder     :            Primary IP
Ucast-Forwarder Status              :               REGULAR

Multicast Information
---------------------

QoS Configuration
-----------------
MetaData QoS (system config)        :                    16 (Effective)

Progress Information
--------------------
Number of jobs completed            :                     0
Has incomplete jobs                 :                    No

  LOC-LEAD:   This SE is the location leader for this delivery service
   REGULAR:   This SE is not the location leader for this delivery service
      LLMT:   This SE cannot find forwarder because this SE has limit on
              the forwarder lookup level
      FAIL:   This SE cannot find forwarder because there is failed SE along
              the path within specified forwarder lookup level
      NGWT:   This SE cannot find forwarder because there is SE with negative
              forwarder-load-weight along the path within the specified
              forwarder lookup level
      LIVE:   The specified delivery service is live delivery service, forwarder not
applicable
         *:   MetaData forwarder and Unicast forwarder are different
```

Note The Has Unfinished Job line is only available if the SE is *not* a Content Acquirer. It is only available on a receiver SE.

The following example provides the forwarder list information for delivery service ID 6290:

```
ServiceEngine# show distribution forwarder-list delivery-service-id 6290 detail
************************* delivery service     6290 ***************************Topology
Information:
  Delivery Service  : (    6290) akot1
  Content Origin    : (    6289) ako
  Home SE           : (    6162) W14-CDE205-1
  Home Location     : (    6189) W14-CDE205-1-location
  Content Acquirer  : (    6181) W14-612-1
  Root Location     : (    6182) W14-612-1-location
```

```
====================== Forwarder Result Start ======================
Latest information for unicast Meta-Data reception
               and for unicast Data reception.

USABLE Forwarder:
  SE ID             : (    6181) W14-612-1
  SE Location       : (    6182) W14-612-1-location
  SE IP address     : 114.0.92.11 SE Fowarder Level : 2
  SE attributes     : resides in root location
                      is the Content Acquirer for the Delivery Service
  SE state          : USABLE
                      applies until Thu Jul  8 05:42:43 2010
  Result Status     :
                      Am Location Leader               : Yes

POLLABLE Forwarder:
  None.

------------------------------------------------------------------------
Location Path:
    List of locations from Home-Location to Root-Location
    Number of locations : 3
        (    6189) W14-CDE205-1-location
        (    6068) L1
        (    6182) W14-612-1-location
    ------------------------------------------------------------------
    List of Delivery-Service-subscribed locations from Home-Location to Root-Location
    Number of locations : 3
        (    6189) W14-CDE205-1-location
        (    6068) L1
        (    6182) W14-612-1-location
------------------------------------------------------------------------
Forwarder Lists:
Location W14-CDE205-1-location(6189) REACHABLE.

    Showing Forwarder list for
        Location : (    6189) W14-CDE205-1-location
        Number of forwarders in location : 1
        ----------------------------------------
        Configured Forwarder SE List:
          <EMPTY>
        Non-configured Forwarder SE List:
          <EMPTY>
    ------------------------------------------------------------------
Location L1(6068) REACHABLE.

    Showing Forwarder list for
        Location : (    6068) L1
        Number of forwarders in location : 0
        ----------------------------------------
        Configured Forwarder SE List:
          <EMPTY>
        Non-configured Forwarder SE List:
          <EMPTY>
    ------------------------------------------------------------------
Location W14-612-1-location(6182) REACHABLE.

    Showing Forwarder list for
        Location : (    6182) W14-612-1-location
        Number of forwarders in location : 1
        ----------------------------------------
        Configured Forwarder SE List:
          SE ID (    6181) W14-612-1  IP 114.0.92.11  state USABLE (Content Origin)
```

```
Non-configured Forwarder SE List:
  <EMPTY>
```

Related Commands

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.
distribution	Reschedules and refreshes content redistribution for a specified delivery service ID or name
show statistics distribution	Displays the statistics of the content distribution components.

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.

Command 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 Internet Streamer CDS software that runs on the device after reload.

Note If you update the CDS 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
CDS software version (disk-based code): CDS-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 2-38 describes the fields shown in the **show flash** display.

Table 2-38 show flash Field Descriptions

Field	Description
Internet Streamer CDS software version (disk-based code)	Internet Streamer CDS 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 2-38 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 flash-media-streaming

To display the Flash Media Streaming information, use the **show flash-media-streaming** command in EXEC configuration mode.

On the SE:

show flash-media-streaming [**license** | **logging** *name* | **mtrack** | **stream-status** {**dvrcast** [**all** *name*] | **live** [**all** *name*]}]

On the SR:

show flash-media-streaming

Syntax Description

license	(Optional) Shows the Flash Media Streaming licenses.
logging	(Optional) Sets the Tar Flash Media Streaming transaction logs to /local/local1/filename.tar.gz.
name	(Optional) Filename.
mtrack	(Optional) Displays the Flash Media Streaming memory usage.
stream-status	(Optional) Displays the Flash Media Streaming stream status.
dvrcast	Displays dvrcast stream status.
all	(Optional) Dumps detail statistics into /local/local1/filename.
live	(Optional) Displays the live stream status.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

When you execute the **show flash-media-streaming stream-status live** command and the Forwarder is a Content Origin server running Linux, the **show** command does not show statistics for the Content Origin server.

Examples

The following example shows how to display the Flash Media Streaming information:

```
ServiceEngine# show flash-media-streaming
Flash Media Streaming is disabled.
Max. Allowed concurrent sessions are 200.
Flash Media Streaming Monitoring is enabled.
Admin list allow: 1.1.1.1
Total number of wholesale licenses is 0.
Bandwidth Details:
Non wholesale bandwidth (Perpetual) is 200000 kbps.
Configured max bandwidth is 10000 kbps.
Total wholesale bandwidth (Term Based) is 0 kbps.
Allowed bandwidth is 10000 kbps.
ServiceEngine#
```

Related Commands

Command	Description
flash-media-streaming	Enables and configures Flash Media Streaming.
show statistics flash-media-streaming	Displays the statistics for Flash Media Streaming.

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.

Command 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.
```

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 DMI[1].
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.

1. Desktop Management Interface

Command 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 2-39 describes the fields shown in the **show hardware** display.

Table 2-39 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.

Table 2-39 show hardware Field Descriptions (continued)

Field	Description
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.
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	

Table 2-39 show hardware Field Descriptions (continued)

Field	Description
SUnreclaim	
KernelStack	
PageTables	
NFS_Unstable	
Bounce	
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
Content Delivery System Software (CDS)
Copyright (c) 1999-2011 by Cisco Systems, Inc.
Content Delivery System Software Release 2.6.0 (build
b460 Aug 28 2011)
Version: cde220-2g2-DEVELOPMENT[vcn-build1:/auto/v
cn-u1/cdsis_release_builds/cdsis_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.

Command 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 2-40 describes the fields shown in the **show hosts** display.

Table 2-40 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 DNS[1] name server or servers.
Host Table	
hostname	FQDN[2] (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.

1. DNS = Domain Name Server
2. FQDN = fully qualified domain name

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 (/).

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-41 describes the fields shown in the **show interface GigabitEthernet** display.

Table 2-41 show interface GigabitEthernet Field Descriptions

Field	Description
Type	Type of interface. Always Ethernet.
Ethernet address	Layer 2 MAC address.
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.

Table 2-41 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 2-42 describes the fields shown in the **show interface PortChannel** display.

Table 2-42 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 2-42 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 2-43 describes the fields shown in the **show interface standby** display.

Table 2-43 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 2-43 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 2-44 describes the fields shown in the **show interface TenGigabitEthernet** display.

Table 2-44 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.

Command 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 unique device identifier (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 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 2-45 describes the fields shown in the **show inventory** display.

Table 2-45 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 access-list

To display the access lists that are defined and applied to specific interfaces or applications, use the **show ip access-list** command in EXEC configuration mode.

show ip access-list [*acl_name* | *acl_num*]

Syntax Description

acl_name	(Optional) Information for a specific access list, using an alphanumeric identifier up to 30 characters, beginning with a letter.
acl_num	(Optional) Information for a specific access list, using a numeric identifier (0 to 99 for standard access lists and 100 to 199 for extended access lists).

Command Defaults

Displays information about all defined access lists.

Command Modes

EXEC configuration mode.

Usage Guidelines

Use the **show ip access-list** command in EXEC configuration mode to display the access lists that have been defined on the current system. Unless you identify a specific access list by name or number, the system displays information about all the defined access lists, including the following sections:

- Available space for new lists and conditions
- Defined access lists
- References by interface and application

Examples

The following example shows sample output from the **show ip access-list** command:

```
ServiceEngine# show ip access-list
Space available:
    47 access lists
   492 access list conditions

Standard IP access list 1
  1 permit 10.1.1.2
  2 deny   10.1.2.1
    (implicit deny any: 2 matches)
  total invocations: 2
Extended IP access list 100
  1 permit tcp host 10.1.1.1 any
  2 permit tcp host 10.1.1.2 any
  3 permit tcp host 10.1.1.3 any
    (implicit fragment permit: 0 matches)
    (implicit deny ip any any: 0 matches)
  total invocations: 0
Standard IP access list test
  1 permit 1.1.1.1 (10 matches)
  2 permit 1.1.1.3
  3 permit 1.1.1.2
    (implicit deny: 2 matches)
  total invocations: 12
```

```
Interface access list references:
  GigabitEthernet 0/0  inbound   100

Application access list references:
  tftp_server                     standard  1
    UDP ports:    69
```

The following example shows sample output from the **show ip access-list** command for the access list named test:

```
ServiceEngine# show ip access-list test
Standard IP access list test
  1 permit 1.1.1.1 (10 matches)
  2 permit 1.1.1.3
  3 permit 1.1.1.2
    (implicit deny: 2 matches)
  total invocations: 12
```

Note The system displays the number of packets that have matched a condition statement only if the number is greater than zero.

Related Commands

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.
ip access-list	Creates and modifies access lists for controlling access to interfaces or applications.

show ip bgp

To display the contents of a particular host in the BGP routing table, use the **show ip bgp** user command in user EXEC configuration mode.

show ip bgp {*ip_address* | *prefix*/*prefix_length*}

Syntax Description

ip_address	(Optional) IP address entered to filter the output to display only a particular host in the 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 Defaults

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 ip bgp all

To display the contents of the BGP routing table, use the **show ip bgp** user command in user EXEC configuration mode.

show ip bgp {*ip_address* | *prefix*/*prefix_length* | **all**}

Syntax Description

ip_address	(Optional) IP address entered to filter the output to display only a particular host in the 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.
all	(Optional) Displays all BGP routes received by the Proximity Engine.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following example is sample output from the **show ip bgp** command. The output shows the contents of the BGP routing table:

```
ServiceRouter# show ip bgp all

BGP table version is 810399, local router ID is 172.20.168.47
Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history,*-valid, >-best
Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist
Origin codes: I - IGP, E - EGP, ? - incomplete

   Network            Next Hop            Metric     LocPrf   Weight Path
   *>i5.5.5.5/32         192.168.86.3             20         100    0 ?
   *>i12.1.1.1/32        192.168.86.3             20         100    0 ?
   *>i13.1.1.1/32        192.168.86.3             20         100    0 ?
   *>i14.1.1.1/32        192.168.86.3             20         100    0 ?
   *>i22.22.22.22/32     192.168.86.3             20         100    0 ?
   *>i40.1.1.0/24        192.168.86.3              0         100    0 ?
   *>i41.1.1.0/24        192.168.86.3              0         100    0 ?
   *>i42.1.1.0/24        192.168.86.3              0         100    0 ?
   *>i43.1.1.0/24        192.168.86.3              0         100    0 ?
*>i45.1.1.0/24         192.168.86.3             0         100    0 ?
-- More --
```

Related Commands

Command	Description
clear ip bgp all	Clears all BGP neighbors.
router bgp	Configures a BGP routing process.

show ip bgp community

To display BGP routes that match a specified BGP community string, use the **show ip bgp community** user EXEC command.

show ip bgp community *community_string*

Syntax Description

community_string	Community string for which to display BGP routes.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

The **show ip bgp community** command is used to display BGP route information for a specified community string. To determine whether a community string exists in the BGP table, use the **show ip bgp summary** command. This command requires a Proximity Engine license.

The **show ip bgp community** command displays the origin AS and community values. Since the community list may be long, the output is limited to 80 columns. Other community unrelated fields longer display in this command; use the **show ip bgp all** command to display these fields.

Examples

In the following example, **show ip bgp summary** output can be used to determine that a community string 100:50 exists in the BGP table. The **show ip bgp community** command displays BGP route information for the community string 100:50. In this example, no route information is present for the community string 100:50:

```
ServiceRouter# show ip bgp summary
BGP router identifier 1.100.8.92, local AS number 23
BGP table version is 2, IPv4 Unicast config peers 2, capable peers 0
0 network entries and 0 paths using 0 bytes of memory
BGP attribute entries [ 0/0 ] , BGP AS path entries [ 0/0 ]
BGP community entries [ 0/0 ] , BGP clusterlist entries [ 0/0 ]
BGP Location Communities: 100:50-100:100

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd

192.168.82.1    4    23       0       0        0    0    0    4d10h Idle
192.168.82.10   4   100       0       0        0    0    0    4d10h Idle

ServiceRouter# show ip bgp community 100:50

BGP table version is 2, local router ID is 1.100.8.92
Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid, >-best

Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist
Origin codes: I - IGP, E - EGP, ? - incomplete

   Network            Next Hop            Metric     LocPrf     Weight Path
ServiceRouter#
```

The following example shows the output for the **show ip bgp community** command:

```
ServiceRouter# show ip bgp community
sh ip bgp community
BGP table version is 32, local router ID is 1.100.9.206
Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid, >-best
Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist
Community: @ - source, # - target

   Network            Next Hop        Origin AS  Community List
*>e2.4.1.0/24         192.168.82.2    33
*>e3.1.4.0/24         192.168.82.2    23         @23:999
*>e5.5.5.5/32         192.168.82.2    23         @23:999
*>e12.1.1.0/24        192.168.82.1    23
*>e12.1.1.1/32        192.168.82.2    23         @23:100 @#44:100
*>e13.1.1.0/24        192.168.82.1    23
*>e13.1.1.1/32        192.168.82.2    23         @#44:100
*>e14.1.1.1/32        192.168.82.2    23         @#44:100
*>e40.1.1.0/24        192.168.82.2    23         @23:999
*>e41.1.1.0/24        192.168.82.2    23         @23:999
*>e42.1.1.0/24        192.168.82.2    33
*>e43.1.1.0/24        192.168.82.2    33
*>e44.1.1.0/24        192.168.82.2    33
*>e45.1.1.0/24        192.168.82.2    33
*>e46.1.1.0/24        192.168.82.2    33
*>e50.1.1.0/24        192.168.82.2    23         @23:999
*>e51.1.1.0/24        192.168.82.2    23         @23:999
*>e52.1.1.0/24        192.168.82.2    33
*>e53.1.1.0/24        192.168.82.2    33
*>e54.1.1.0/24        192.168.82.2    33
*>e55.1.1.0/24        192.168.82.2    33
*>e62.1.1.1/32        192.168.82.2    23         @23:999
*>e62.62.62.0/24      192.168.82.2    23         @23:999
*>e108.0.32.0/24      192.168.82.2    33
*>e171.70.0.0/16      192.168.82.2    33
*>e171.71.0.0/16      192.168.82.2    33
*>e172.20.0.0/16      192.168.82.2    33
*>e192.168.81.0/24    192.168.82.2    23
*>e203.0.0.205/32     192.168.82.2    23         @23:999
ServiceRouter#
```

Related Commands

Command	Description
location community	BGP location-specific community configuration.
router bgp	Configures a BGP routing process.

show ip bgp ipv4 unicast

To display information relating to all IPv4 unicast routes in the BGP routing table, use the **show ip bgp ipv4 unicast** user command in user EXEC configuration mode.

show ip bgp ipv4 unicast

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

The **show ip bgp ipv4 unicast** command is used to display information relating to all IPv4 unicast routes in the BGP routing table. To see any route in the output of this command, BGP needs to connect successfully to at least one neighbor and receive route information from this neighbor. This command requires a Proximity Engine license.

Examples

The following is sample output from the **show ip bgp ipv4 unicast** command:

```
ServiceRouter# show ip bgp ipv4 unicast

BGP table version is 810674, local router ID is 172.20.168.47
Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid, >-best

Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist
Origin codes: I - IGP, E - EGP, ? - incomplete

   Network            Next Hop            Metric     LocPrf     Weight Path
*>i5.5.5.5/32         192.168.86.3            20        100          0 ?
*>i12.1.1.1/32        192.168.86.3            20        100          0 ?
*>i13.1.1.1/32        192.168.86.3            20        100          0 ?
*>i14.1.1.1/32        192.168.86.3            20        100          0 ?
*>i22.22.22.22/32     192.168.86.3            20        100          0 ?
*>i40.1.1.0/24        192.168.86.3             0        100          0 ?
*>i41.1.1.0/24        192.168.86.3             0        100          0 ?
*>i42.1.1.0/24        192.168.86.3             0        100          0 ?
*>i43.1.1.0/24        192.168.86.3             0        100          0 ?
*>i44.1.1.0/24        192.168.86.3             0        100          0 ?
*>i45.1.1.0/24        192.168.86.3             0        100          0 ?
*>i50.1.1.0/24        192.168.86.3             0        100          0 ?
*>i51.1.1.0/24        192.168.86.3             0        100          0 ?
-- More --
```

Related Commands

Command	Description
clear ip bgp all	Clears all BGP neighbors.
router bgp	Configures a BGP routing process.

show ip bgp memory

To display memory usage information of the running BGP daemon, use the **show ip bgp memory** user command in user EXEC configuration mode.

show ip bgp memory

Syntax Description

This command has no keywords or arguments.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following example is sample output from the **show ip bgp memory** command:

```
ServiceRouter# show ip bgp memory

Shared memory information for /topos_shm_bgp,
Current-Size         HWM    Maximum-Size
      1727064     1727088       209715200


BGP memory usage stats

Private memory
Total mallocs/frees/failed : 31/9/0
Memory allocated           : 4258692 bytes
HWM allocated              : 4262700 bytes

Shared memory
Total mallocs/frees/failed : 19/3/0
Memory requested/allocated : 1534799/1727064 bytes
HWM requested/allocated    : 1534819/1727088 bytes

ServiceRouter#
```

Related Commands

Command	Description
router bgp	Configures a BGP routing process.

show ip bgp neighbors

To display information about the TCP and BGP connections to neighbors, use the s**how ip bgp neighbors** user command in user EXEC configuration mode.

show ip bgp neighbors [*ip_address*]

Syntax Description

ip_address	(Optional) IP address of a neighbor.

Command Defaults

The output of this command displays information for all neighbors for IPv4 address family sessions only.

Command Modes

User EXEC configuration mode.

Usage Guidelines

The **show ip bgp neighbors** command is used to display BGP and TCP connection information for neighbor sessions. For BGP, this includes detailed neighbor attribute, capability, path, and prefix information. For TCP, this includes statistics related to BGP neighbor session establishment and maintenance.

This command requires a Proximity Engine license.

Examples

The following example is sample output from the **show ip bgp neighbors** command. The example shows the 192.168.86.3 neighbor. This neighbor is an internal BGP (iBGP) peer. This neighbor supports the route refresh and graceful restart capabilities.

```
ServiceRouter# show ip bgp neighbors
BGP neighbor is 48.0.0.8, remote AS 2, ebgp link, Peer index 1
BGP version 4, remote router ID 48.0.0.8
BGP state = Established, up for 00:00:04
Peer is directly attached, interface GigabitEthernet 2/0
Last read 0.027030, hold time = 180, keepalive interval is 60 seconds
Last written 00:00:01, keepalive timer expiry due 00:00:58
Received 14265 messages, 0 notifications, 0 bytes in queue
Sent 5 messages, 0 notifications, 0 bytes in queue
Connections established 1; dropped 0
Last reset by us never, due to process restart
Last reset by peer never, due to process restart

Neighbor capabilities:
Dynamic capability: advertised (mp, refresh, gr)
Dynamic capability (old): advertised
Address family IPv4 Unicast: advertised

Capabilities parameter not sent by neighbor
Exchanging IPv4 Unicast NLRI by default

For address family: IPv4 Unicast
BGP table version 1, neighbor version 101573
142640 accepted paths consume 5135040 bytes of memory
0 sent paths

Local host: 48.0.0.4, Local port: 179
```

```
Foreign host: 48.0.0.8, Foreign port: 2867
fd = 42

ServiceRouter#
```

To display information for all BGP neighbors, use the **show ip bgp neighbors** command. In this example, the Proximity Engine has two BGP peers, 192.168.86.3 and 192.168.86.87.

```
ServiceRouter# show ip bgp neighbors

BGP neighbor is 192.168.86.3,  remote AS 23, ibgp link,  Peer index 1
  BGP version 4, remote router ID 192.168.86.3
  BGP state = Established, up for 1d05h
  Peer is directly attached, interface GigabitEthernet 2/0
  Last read 0.868226, hold time = 180, keepalive interval is 60 seconds
  Last written 00:00:09, keepalive timer expiry due 00:00:50
  Received 78444 messages, 0 notifications, 0 bytes in queue
  Sent 1788 messages, 0 notifications, 0 bytes in queue
  Connections established 1; dropped 0
  Last reset by us never, due to process restart
  Last reset by peer never, due to process restart

  Neighbor capabilities:
  Dynamic capability: advertised (mp, refresh, gr)
  Dynamic capability (old): advertised
  Route refresh capability (new): advertised received
  Route refresh capability (old): advertised received
  Address family IPv4 Unicast: advertised received

  For address family: IPv4 Unicast
  BGP table version 1, neighbor version 810749
  8518 accepted paths consume 613296 bytes of memory
  0 sent paths

  Local host: 192.168.86.47, Local port: 58920
  Foreign host: 192.168.86.3, Foreign port: 179
  fd = 35

BGP neighbor is 192.168.86.87,  remote AS 23, ibgp link,  Peer index 2
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle, down for 00:00:10
  Last read never, hold time = 180, keepalive interval is 60 seconds
  Last written never, keepalive timer not running
  Received 0 messages, 0 notifications, 0 bytes in queue
  Sent 0 messages, 0 notifications, 0 bytes in queue
  Connections established 0; dropped 0
  Last reset by us never, due to process restart
  Last reset by peer never, due to process restart

  For address family: IPv4 Unicast
  BGP table version 1, neighbor version 0
  0 accepted paths consume 0 bytes of memory
  0 sent paths

No established BGP session with peer
```

Related Commands

Command	Description
clear ip bgp all	Clears all BGP neighbors.
router bgp	Configures a BGP routing process.

show ip bgp nexthop-database

To display the next-hop database information in the BGP routing table, use the **show ip bgp nexthop-database** user command in user EXEC configuration mode.

show ip bgp nexthop-database

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

The **show ip bgp nexthop-database** command is used to display the BGP next-hop information, including IGP cost, IGP route type, IGP preference, interface to reach this next-hop, time of last next-hop resolution, and reachability. This command requires a Proximity Engine license.

Examples

The following example is sample output from the **show ip bgp nexthop-database** command:

```
ServiceRouter# show ip bgp nexthop-database

Nexthop: 192.168.86.3, Refcount: 4021, IGP cost: 0
IGP Route type: 0, IGP preference: 0
Attached nexthop: 192.168.86.3, Interface: GigabitEthernet 2/0
Nexthop is attached not-local reachable
Nexthop last resolved: 1d05h, using 192.168.86.0/24
Metric next advertise: Never

ServiceRouter#
```

Related Commands

Command	Description
router bgp	Configures a BGP routing process.
show ip bgp all	Displays BGP route table information.

show ip bgp summary

To display the status of all BGP connections, use the **show ip bgp summary** user command in user EXEC configuration mode.

show ip bgp summary

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

The **show ip bgp summary** command is used to display BGP path, prefix, and attribute information for all connections to BGP neighbors.

A *path* is a route to a given destination. By default, BGP only installs a single path for each destination. If multipath routes are configured, BGP installs a path for each multipath route, and only one multipath route is marked as the best path. A prefix is an IP address and network mask. It can represent an entire network, a subset of a network, or a single host route.

BGP attribute and cache entries are displayed individually and in combinations that affect the best path selection process. The fields for this output are displayed when the related BGP feature is configured or when the BGP attribute is received. Memory usage is displayed in bytes.

This command requires a Proximity Engine license.

Examples

The following example is sample output from the **show ip bgp summary** command:

```
ServiceRouter# show ip bgp summary

BGP router identifier 1.100.8.40, local AS number 65204
BGP table version is 567, IPv4 Unicast config peers 1, capable peers 1
80 network entries and 80 paths using 16960 bytes of memory
BGP attribute entries [ 10/1600 ] , BGP AS path entries [ 10/174 ]
BGP community entries [ 10/160 ] , BGP clusterlist entries [ 0/0 ]
location community 100:1535 200:4566 123:3000-123:4000 350:2530 300:500-300:1000

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.52.10   4 65204    4363    4289      567    0    0 00:00:59 80

ServiceRouter#
```

Related Commands

Command	Description
router bgp	Configures a BGP routing process.
show ip bgp all	Displays BGP route table information.

show ip interface

To display the IP interface state and address/mask for all interfaces, use the **show ip interface** command in user EXEC configuration mode.

show ip interface

Syntax Description

brief	Displays a summary of the IP interface status and configuration.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command is used to display a Summary of the IP interface status and configuration.

Examples

The following example is sample output from the **show ip bgp summary** command:

```
ServiceRouter# show ip interface brief

Interface            IP Address      Interface Status
PortChannel 1        3.1.14.71       protocol-up/link-up/admin-up
PortChannel 2        4.0.8.12        protocol-up/link-up/admin-up

ServiceRouter#
```

show ip ospf

To display general information about OSPF routing processes, use the **show ip ospf** command in privileged EXEC configuration mode.

show ip ospf

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show ip ospf** command:

```
ServiceRouter# show ip ospf

OSPF information:
 Routing Process p1 with ID 172.20.168.41 context default
 Stateful High Availability enabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Reference Bandwidth is 40000 Mbps
 Initial Inter-SPF schedule delay 200.000 msecs,
   backoff factor 2, capped at 1000.000 msecs,
   minimum Inter-SPF delay reset after 5000.000 msecs
 Minimum hold time for Router LSA throttle 5000.000 ms
 Minimum hold time for Network LSA throttle 5000.000 ms
 Minimum LSA arrival 1000.000 msec
 Maximum paths to destination 8
 Originating router LSA with maximum metric
   Condition: Always
 Number of external LSAs 22, checksum sum 0xdc4ba
 Number of opaque AS LSA 0, checksum sum 0
 Number of areas is 1, 1 normal, 0 stub, 0 nssa
 Number of active areas is 1, 1 normal, 0 stub, 0 nssa
   Area BACKBONE(0)
        Area has existed for 00:00:02
        Interfaces in this area: 1 Active interfaces: 1
        No authentication available
        SPF calculation has run 2 times
         Last SPF ran for 0.000054s
        Router LSA throttle timer due in 00:00:02
        Area ranges are
        Number of LSAs: 498, checksum sum 0xf5eb6b

ServiceRouter#
```

Table 2-46 describes the significant fields included in the display above.

Table 2-46 Significant fields included in output of show ip ospf command

Field	Description
Routing Process p1 with ID 172.20.168.41	Process ID p1 and OSPF router ID 172.20.168.41 (IP address of Proximity Engine). For Proximity Engine, p1 cannot be changed.
Supports …	Number of types of service supported (Type 0 only).
Summary Link update interval	Specifies summary update interval in hours:minutes:seconds, and time until next update.
External Link update interval	Specifies external update interval in hours:minutes:seconds, and time until next update.
Redistributing External Routes from	Lists of redistributed routes, by protocol.
Number of areas	Number of areas in router, area addresses, and so on.
Link State Update Interval.	Specifies router and network link-state update interval in hours:minutes:seconds, and time until next update.
Link State Age Interval	Specifies max-aged update deletion interval, and time until next database cleanup, in hours:minutes:seconds.
SPF Calculation	Number of times SPF calculation is done.

Related Commands

Command	Description
router ospf	Enables the OSPF routing process.

show ip ospf border-routers

To display general information about OSPF border routers, use the **show ip ospf border-routers** command in privileged EXEC configuration mode.

show ip ospf border-routers

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show ip ospf** command:

```
ServiceRouter# show ip ospf border-routers
OSPF Process ID p1 context default, Internal Routing Table
Codes: i - Intra-area route, I - Inter-area route

intra 192.168.0.86 [65535], ASBR, Area 0, SPF 3
     via 192.168.86.3, GigabitEthernet 2/0
```

Related Commands

Command	Description
router ospf	Enables the OSPF routing process.

show ip ospf database

To display lists of information related to the OSPF database for a specific router, use the **show ip ospf database** user command in EXEC configuration mode. The various forms of this command deliver information about different OSPF link-state advertisements (LSAs).

show ip ospf database [**adv-router** [*ip_address*]] [**detail**] | [**asbr-summary**] [*link_state_id*] [**detail**] | [**database-summary**] | [**detail**] | [**external**] [*link_state_id*] [**detail**] | [**network**] [*link_state_id*] [**detail**] | [**nssa-external**] [*link_state_id*] [**detail**] | [**router**] [*link_state_id*] [**detail**] | [**self-originate**] [**detail**] | [**summary**] [*link_state_id*] [**detail**]

Syntax Description

adv-router [*ip_address*]	(Optional) Displays all the link-state advertisements (LSAs) of the specified router. If no IP address is included, the information displayed relates to the local router (in this case, the same as the **self-originate** keyword).
asbr-summary	(Optional) Displays information about only the Autonomous System Boundary Router (ASBR) summary LSAs.
link_state_id	(Optional) Portion of the Internet environment that is being described by the advertisement. The value entered depends on the type of the LSA. The value must be entered in the form of an IP address. When the LSA is describing a network, the *link_state_id* argument can take one of two forms: • Network IP address (as in Type 3 summary link advertisements and in autonomous system external link advertisements). • Derived address obtained from the link-state ID. (Note that masking a network links the advertisement link-state ID with the network subnet mask yielding the network IP address.) When the LSA is describing a router, the link-state ID is always the OSPF router ID of the described router. When an autonomous system external advertisement (Type 5) is describing a default route, its link-state ID is set to the default destination (0.0.0.0).
database-summary	(Optional) Displays how many of each type of LSA for each area there are in the database, and displays the total.
detail	(Optional) Displays LSA in detail.
external	(Optional) Displays information only about the external LSAs.
network	(Optional) Displays information only about the network LSAs.
nssa-external	(Optional) Displays information only about the Not-So-Stubby Area (NSSA) external LSAs.
router	(Optional) Displays information only about the router LSAs.
self-originate	(Optional) Displays only self-originated LSAs (from the local router).
summary	(Optional) Displays information only about the summary LSAs.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show ip ospf database** command when no arguments or keywords are used:

```
ServiceRouter# show ip ospf database
    OSPF Router with ID (172.20.168.88) (Process ID p1 context default)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#     Checksum Link Count
172.20.168.88   172.20.168.88   1686        0x80000006 0x4531   1
192.168.0.4     192.168.0.4     1284        0x8000000a 0x80cf   1

                Network Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
192.168.20.2    192.168.0.4     1284        0x80000003 0x49d2

ServiceRouter#
```

Table 2-47 describes the significant fields included in the display above.

Table 2-47 Significant fields included in output of show ip ospf database

Field	Description
Link ID	Router ID number.
ADV Router	Advertising router ID.
Age	Link-state age.
Seq#	Link-state sequence number (detects old or duplicate LSAs).
Checksum	Fletcher checksum of the complete contents of the LSA
Link count	Number of interfaces detected for router.

The following is sample output from the **show ip ospf database** command with the **asbr-summary** keyword:

```
ServiceRouter# show ip ospf database asbr-summary
    OSPF Router with ID (172.20.168.41) (Process ID p1 context default)

                Summary ASBR Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
193.0.50.3      193.0.50.3      1281        0x800007a8 0x86d4
193.0.150.3     193.0.150.3     1281        0x800007ac 0x6f1f

                Summary ASBR Link States (Area 10)

Link ID         ADV Router      Age         Seq#       Checksum
193.0.50.3      172.20.168.41   345         0x8000002a 0x0a95
193.0.150.3     172.20.168.41   345         0x8000002a 0xb981

ServiceRouter#
```

Table 2-48 describes the significant fields included in the display above.

Table 2-48 Significant fields included in output of show ip ospf database asbr-summary

Field	Description
Link ID	Router ID number.
ADV Router	Advertising router ID.
Age	Link-state age.
Seq#	Link-state sequence number (detects old or duplicate LSAs).
Checksum	Fletcher checksum of the complete contents of the LSA.

The following is sample output from the **show ip ospf database** command with the **external** keyword:

```
ServiceRouter# show ip ospf database external

        OSPF Router with ID (172.20.168.41) (Process ID p1 context default)

                Type-5 AS External Link States

Link ID         ADV Router      Age         Seq#       Checksum Tag
30.0.0.0        193.0.50.3      1580        0x800007ab 0x7e24    0
30.0.0.0        193.0.150.3     1580        0x800007ae 0xb981    0
30.0.1.0        193.0.50.3      1580        0x800007ab 0x732e    0
30.0.1.0        193.0.150.3     1580        0x800007ae 0xae8b    0
30.0.2.0        193.0.50.3      1580        0x800007ab 0x6838    0
30.0.2.0        193.0.150.3     1580        0x800007ae 0xa395    0
30.0.3.0        193.0.50.3      1580        0x800007ab 0x5d42    0
30.0.3.0        193.0.150.3     1580        0x800007ae 0x989f    0

ServiceRouter#
```

Table 2-49 describes the significant fields included in the display above.

Table 2-49 Significant fields included in output of show ip ospf database external

Field	Description
Link ID	Router ID number.
ADV Router	Advertising router ID.
Age	Link-state age.
Seq#	Link-state sequence number (detects old or duplicate LSAs).
Checksum	Fletcher checksum of the complete contents of the LSA.
Tag	External route tag, a 32-bit field attached to each external route. This is not used by the OSPF protocol itself.

The following is sample output from the **show ip ospf database** command with the **network** keyword:

```
ServiceRouter# show ip ospf database network

    OSPF Router with ID (172.20.168.41) (Process ID p1 context default)

                Network Link States (Area 0)
```

```
Link ID         ADV Router      Age         Seq#       Checksum
192.168.78.4    100.73.1.4      312         0x80000135 0xeaeb
192.168.82.4    100.73.1.4      1311        0x8000009b 0xbc01
193.0.50.2      193.0.50.3      57          0x800007ad 0x7cec
193.0.61.2      193.0.61.3      57          0x80000fe4 0x0d5e
193.0.72.2      193.0.72.3      57          0x80000fe4 0x3906
193.0.83.2      193.0.83.3      57          0x800007a9 0xf362
193.0.84.2      193.0.83.3      57          0x800007a9 0xc9a1

ServiceRouter#
```

Table 2-50 describes the significant fields included in the display above.

Table 2-50 Significant fields included in output of show ip ospf database network

Field	Description
Link ID	Router ID number.
ADV Router	Advertising router ID.
Age	Link-state age.
Seq#	Link-state sequence number (detects old or duplicate LSAs).
Checksum	Fletcher checksum of the complete contents of the LSA.

The following is sample output from the **show ip ospf database** command with the **router** keyword:

```
ServiceRouter# show ip ospf database router

        OSPF Router with ID (172.20.168.41) (Process ID p1 context default)

                Router Link States (Area 0)

Link ID         ADV Router      Age      Seq#       Checksum Link Count
1.1.78.8        1.1.78.8        525      0x800007af 0x801b   2
1.1.78.9        1.1.78.9        525      0x800007ab 0x7ce8   2
100.73.1.4      100.73.1.4      780      0x800003bd 0x2dd9   2
172.20.168.41   172.20.168.41   1388     0x80000030 0x67fa   1
172.20.168.83   172.20.168.83   1179     0x80000039 0xfddd   1
192.168.82.1    192.168.82.1    1299     0x8000006f 0x06fe   2

                Router Link States (Area 10)

Link ID         ADV Router      Age      Seq#       Checksum Link Count
172.20.168.41   172.20.168.41   628      0x8000002c 0xf99d   1

ServiceRouter#
```

Table 2-51 describes the significant fields included in the display above.

Table 2-51 Significant fields included in output of show ip ospf database router

Field	Description
Link ID	Router ID number.
ADV Router	Advertising router ID.
Age	Link-state age.
Seq#	Link-state sequence number (detects old or duplicate LSAs).

Table 2-51 Significant fields included in output of show ip ospf database router (continued)

Field	Description
Checksum	Fletcher checksum of the complete contents of the LSA.
Link count	Number of interfaces detected for router.

The following is sample output from the **show ip ospf database** command with the **summary** keyword:

```
ServiceRouter# show ip ospf database summary

        OSPF Router with ID (172.20.168.41) (Process ID p1 context default)

                Summary Network Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
20.0.0.0        193.0.50.3      1325        0x800007ac 0xa496
20.0.0.0        193.0.150.3     1326        0x800007af 0xdff3
20.0.1.0        193.0.50.3      1325        0x800007ac 0x99a0
20.0.1.0        193.0.150.3     1326        0x800007af 0xd4fd
20.0.2.0        193.0.50.3      1325        0x800007ac 0x8eaa
20.0.2.0        193.0.150.3     1326        0x800007af 0xc908

                Summary Network Link States (Area 10)

Link ID         ADV Router      Age         Seq#       Checksum
192.168.78.0    172.20.168.41   370         0x8000002b 0xc127

ServiceRouter#
```

Table 2-52 describes the significant fields included in the display above.

Table 2-52 Significant fields included in output of show ip ospf database summary

Field	Description
Link ID	Router ID number.
ADV Router	Advertising router ID.
Age	Link-state age.
Seq#	Link-state sequence number (detects old or duplicate LSAs).
Checksum	Fletcher checksum of the complete contents of the LSA.

The following is sample output from the **show ip ospf database** command with the **database-summary** keyword:

```
ServiceRouter# show ip ospf database database-summary

    OSPF Router with ID (172.20.168.41) (Process ID p1 context default)

Area 0 database summary
  LSA Type            Count
  Opaque Link         0
  Router              156
  Network             296
  Summary Network     41
  Summary ASBR        2
  Type-7 AS External  0
  Opaque Area         0
```

```
  Subtotal            495

Area 10 database summary
  LSA Type            Count
  Opaque Link         0
  Router              1
  Network             0
  Summary Network     1
  Summary ASBR        2
  Type-7 AS External  0
  Opaque Area         0
  Subtotal            4

Process p1 database summary
  LSA Type            Count
  Opaque Link         0
  Router              157
  Network             296
  Summary Network     42
  Summary ASBR        4
  Type-7 AS External  0
  Opaque Area         0
  Type-5 AS External  20
  Opaque AS           0
  Total               519

ServiceRouter#
```

Table 2-53 describes the significant fields included in the display above.

Table 2-53 Significant fields included in output of show ip ospf database database-summary command

Field	Description
OSPF Router with id	Router ID number.
Process ID	OSPF process ID (for Proximity Engine, the id is p1)
LSA Type	Link-state type.
Area ID	Area number
Router	Number of router LSAs in that area
Network	Number of network LSAs in that area
Summary Network	Number of summary LSAs in that area
Summary ASBR	Number of summary ASBR LSAs in that area
Subtotal	Sum of Router, Network, Summary Network, and Summary ASBR for that area
AS External	Number of external LSAs.

Related Commands

Command	Description
router ospf	Enables the OSPF routing process.

show ip ospf interface

To display OSPF-related interface information, use the show **ip ospf interface** command in user EXEC configuration mode.

show ip ospf interface

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following example shows how to display sample output from the **show ip ospf interface** command.

```
ServiceRouter# show ip ospf interface

Interface:  GigabitEthernet 1/0 is up, line protocol is up
    IP address 192.168.78.41/24, Process ID p1 context default, area 0
    State BDR, Network type BROADCAST, cost 1
    Index 1, Transmit delay 1 sec, Router Priority 1
    Designated Router ID: 100.73.1.4, address: 192.168.78.4
    Backup Designated Router ID: 172.20.168.41, address: 192.168.78.41
    4 Neighbors, flooding to 2, adjacent with 2
    Timer intervals: Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello timer due in 00:00:01
    No authentication
    Number of link LSAs: 0, checksum sum 0
 GigabitEthernet 1/0 is up, line protocol is up
    IP address 172.20.168.41/24, Process ID p1 context default, area 10
    State DR, Network type BROADCAST, cost 1
    Index 2, Transmit delay 1 sec, Router Priority 1
    Designated Router ID: 172.20.168.41, address: 172.20.168.41
    No backup designated router on this network
    0 Neighbors, flooding to 0, adjacent with 0
    Timer intervals: Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello timer due in 00:00:07
    No authentication
    Number of link LSAs: 0, checksum sum 0

ServiceRouter#
```

Table 2-54 describes the significant fields included in the display above.

Table 2-54 Significant fields included in output of the show ip ospf interface command

Field	Description
Interface	Status of physical link and operational status of the protocol.
IP address	Interface IP address, subnet mask, and area number/address.
State	Interface state (DR – Designated Router, BDR – Backup Designated Router).
Timer intervals configured	Configuration of timer intervals.
Transmit delay	Transmit delay, router priority.
Hello	Number of seconds until next hello packet is sent out this interface.
Neighbor Count	Count of network neighbors and list of adjacent neighbors.

Related Commands

Command	Description
router ospf	Enables the OSPF routing process.

show ip ospf memory

To display memory usage of the OSPF process, use the **show ip ospf memory** command in user EXEC configuration mode.

show ip ospf memory

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following example shows how to display sample output from the **show ip ospf memory** command.

```
ServiceRouter# show ip ospf memory

OSPF memory usage statistics:

Shared memory information for /topos_shm_ospf,
Current-Size         HWM    Maximum-Size
          48     1088240         4194304


 OSPF Process ID p1, Memory statistics
  Byte usage:    needed 0, overhead 0, using 0 bytes
  Allocations:   current 0, created 0, failed 0, free 0
  Bitfields:     current 0, created 0, failed 0, free 0, using 0 bytes
  Slabs:         current 0, created 0, failed 0, free 0, using 8 bytes
  Index failure: Interface 0, Neighbor 0

  CurBytes  Current      HWM   Malloc     Free   Description
       728        1        1        1        0   area
    119712      516      520      526       10   lsdb entry
       320        2        2        2        0   ASBR route
       984        1        1        1        0   ospf interface
        16        1        1        1        0   backup safety memory
     48136      515      520     9465     8950   lsa
        60        1        2        2        1   lsa
         0        0      197      517      517   lsa
         0        0        2        2        2   redist work
   1048576        1        1        1        0   backup memory
      4192        1        1        1        0   ospf subrouter
      2920        1        1        1        0   ager wheel
     10100       11       11       13        2   pak buffer
        80        1        1        1        0   ospf table
        48        1        1        1        0   ager wheel holder
      2784        3        3        3        0   neighbor
        24        1        1        1        0   network configuration entry
```

Related Commands

Command	Description
router ospf	Enables the OSPF routing process.

show ip ospf neighbor

To display OSPF neighbor information, use the **show ip ospf neighbor** command in user EXEC configuration mode.

show ip ospf neighbor [*neighbor_id* | **detail** | **summary**]

Syntax Description

neighbor_id	(Optional) Neighbor ID or Router ID.
detail	(Optional) Displays details of neighbors.
summary	(Optional) Displays a summary of neighbors.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show ip ospf neighbor** command. It shows a single line of summary information for each neighbor:

```
ServiceRouter# show ip ospf neighbors

 OSPF Process ID p1 context default
 Total number of neighbors: 2
 Neighbor ID     Pri State            Up Time  Address         Interface
 100.73.1.4        1 FULL/DR          1d00h    192.168.78.4     GigabitEthernet 1/0
 172.20.168.83     1 FULL/DROTHER     14:42:44 192.168.78.83    GigabitEthernet 1/0

ServiceRouter#
```

The following is sample output showing summary information about the neighbor that matches the specified neighbor ID:

```
ServiceRouter# show ip ospf neighbors 100.73.1.4

 OSPF Process ID p1 context default
 Total number of neighbors: 4
 Neighbor ID     Pri State            Up Time  Address         Interface
 100.73.1.4        1 FULL/DR          1d00h    192.168.78.4     GigabitEthernet 1/0

ServiceRouter#
```

The following is sample output from the **show ip ospf neighbor detail** command:

```
ServiceRouter# show ip ospf neighbors detail

Neighbor 100.73.1.4, interface address 192.168.78.4
    Process ID p1 context default, in area 0 via interface GigabitEthernet 1/0
    State is FULL, 6 state changes, last change 1d00h
    Neighbor priority is 1
```

```
    DR is 192.168.78.4 BDR is 192.168.78.41
    Hello options 0x12, dbd options 0x52
    Last non-hello packet received 0.301737
      Dead timer due in 00:00:40
 Neighbor 172.20.168.83, interface address 192.168.78.83
    Process ID p1 context default, in area 0 via interface GigabitEthernet 1/0
    State is FULL, 4 state changes, last change 14:47:09
    Neighbor priority is 1
    DR is 192.168.78.4 BDR is 192.168.78.41
    Hello options 0x2, dbd options 0x42
    Last non-hello packet received 00:00:08
      Dead timer due in 00:00:34
ServiceRouter#
```

The following is sample output from the **show ip ospf neighbor summary** command:

```
ServiceRouter# show ip ospf neighbors summary

 OSPF Process ID p1 context default, Neighbor Summary
 Interface Down Attempt Init TwoWay ExStart Exchange Loading Full Total
     Total    0       0    0      0       0        0       0    2     2
      GigabitEthernet 1/0    0       0    0      0       0        0       0    2     2

ServiceRouter#
```

Table 2-55 describes the significant fields included in the display above.

Table 2-55 Significant fields included in output of the* show ip ospf neighbor summary *Command

Field	Description
Neighbor	Neighbor router ID.
interface address	IP address of the interface.
in area	Area and interface through which the OSPF neighbor is known.
Neighbor priority	Router priority.
State	OSPF state.
state changes	Number of state changes since the neighbor was created. This value can be reset using the **clear ip ospf neighbor** command.
DR is	Router ID of the designated router for the interface.
BDR is	Router ID of the backup designated router for the interface.
Hello option	Hello packet options field contents (E-bit only).
Dead timer	Expected time before Proximity Engine declares the neighbor dead.
UP Time	Number of hours:minutes:seconds since the neighbor went into 2-way state.
Last non-hello packet	Number of hours:minutes:seconds since the last non-hello packet received

Related Commands

Command	Description
router ospf	Enables the OSPF routing process.

show ip ospf request-list

To display a list of all link-state advertisements (LSAs) requested by a router, use the **show ip ospf request-list** command in EXEC configuration mode.

show ip ospf request-list *neighbor interface*

Syntax Description

neighbor	Neighbor router ID.
interface	Interface name.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The output is useful in debugging OSPF routing operations. This command requires a Proximity Engine license.

Examples

The following example shows how to display sample output from the **show ip ospf request-list** command, with neighbor router ID set to 100.73.1.4, and interface set to 'GigabitEthernet 1/0':

```
ServiceRouter# show ip ospf request-list 100.73.1.4 GigabitEthernet 1/0

 OSPF Process ID p1 context default
 Neighbor 100.73.1.4, interface GigabitEthernet 1/0, address 192.168.78.4
 1 LSAs on request-list

 Type LSID            Adv Rtr         Seq No     Checksum Age
    1 192.168.1.12    192.168.1.12    0x8000020D 0x6572   5

ServiceRouter#
```

Related Commands

Command	Description
router ospf	Enables the OSPF routing process.

show ip ospf retransmission-list

To display a list of all link-state advertisements (LSAs) waiting to be re-sent, use the **show ip ospf retransmission-list** command in EXEC configuration mode.

show ip ospf retransmission-list *neighbor interface*

Syntax Description

neighbor	Neighbor router ID.
interface	Interface name.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

The output of this command is useful in debugging OSPF routing operations. This command requires a Proximity Engine license.

Examples

The following example shows how to display sample output from the **show ip ospf retransmission-list** command, with neighbor router ID set to '100.73.1.4', and interface set to 'GigabitEthernet 1/0':

```
ServiceRouter# show ip ospf retransmission-list 100.73.1.4 GigabitEthernet 1/0

 OSPF Process ID p1 context default
 Neighbor 100.73.1.4, interface GigabitEthernet 1/0, address 192.168.78.4

 Link state retransmission due in 00:00:04
 Type LSID            Adv Rtr         Seq No     Checksum Age
    1 172.20.168.41   172.20.168.41   0x80000044 0x3f0f   0

ServiceRouter#
```

Related Commands

Command	Description
router ospf	Enables the OSPF routing process.

show ip ospf route

To display the OSPF RSPF route for OSPF routes, use the **show ip ospf route** command in EXEC configuration mode.

show ip ospf route [**all** | *router_id*]

Syntax Description

all	(Optional) Displays for all OSPF routes.
router_id	(Optional) Displays for this router ID

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show ip ospf route** command:

```
ServiceRouter# show ip ospf route

 OSPF Process ID p1 context default, Routing Table
  (D) denotes route is directly attached      (R) denotes route is in RIB
20.0.0.0/24 (inter) area 0
     via 192.168.78.8/GigabitEthernet 1/0, cost 65645
     via 192.168.78.9/GigabitEthernet 1/0, cost 65645
20.0.1.0/24 (inter) area 0
     via 192.168.78.8/GigabitEthernet 1/0, cost 65645
     via 192.168.78.9/GigabitEthernet 1/0, cost 65645
20.0.2.0/24 (inter) area 0
     via 192.168.78.8/GigabitEthernet 1/0, cost 65645
     via 192.168.78.9/GigabitEthernet 1/0, cost 65645
20.0.3.0/24 (inter) area 0
     via 192.168.78.8/GigabitEthernet 1/0, cost 65645
     via 192.168.78.9/GigabitEthernet 1/0, cost 65645
20.0.4.0/24 (inter) area 0
     via 192.168.78.8/GigabitEthernet 1/0, cost 65645
     via 192.168.78.9/GigabitEthernet 1/0, cost 65645
20.0.5.0/24 (inter) area 0
     via 192.168.78.8/GigabitEthernet 1/0, cost 65645
     via 192.168.78.9/GigabitEthernet 1/0, cost 65645
20.0.6.0/24 (inter) area 0
     via 192.168.78.8/GigabitEthernet 1/0, cost 65645
     via 192.168.78.9/GigabitEthernet 1/0, cost 65645
192.168.78.0/24 (intra)(D) area 0
     via 192.168.78.41/GigabitEthernet 1/0*, cost 65535
192.168.79.0/24 (intra) area 0
     via 192.168.78.4/GigabitEthernet 1/0, cost 65537
192.168.82.0/24 (intra) area 0
     via 192.168.78.4/GigabitEthernet 1/0, cost 65536
```

Related Commands

Command	Description
router ospf	Enables the OSPF routing process.

show ip ospf rspf route

To display OSPF reverse shortest path first (RSPF) from a specific router(s), use the s**how ip ospf rspf route** command in EXEC configuration mode.

show ip ospf rspf route [*router_id*]

Syntax Description

router_id	(Optional) Router ID.

Command Defaults

If no router ID is specified, displays OSPF RSPF information for all router IDs.

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command shows cached RSPF routing information because of previous proximity request. This command requires a Proximity Engine license.

Examples

The following is sample output from the **show ip ospf rspf route** command:

```
ServiceRouter# show ip ospf rspf route

Advertising Router  SPF Version  Cache Hit       Age
172.20.168.41          2292         1        00:00:04

ServiceRouter#
```

Table 2-56 describes the significant fields included in the display above

Table 2-56 Significant fields included in output of the show ip ospf rspf router command

Field	Description
Advertising Router	Rspf is computed based on this router.
SPF version	SPF version.
Cache Hit	Same proximity request received (Cache hit + 1) times before has been cache expired.
Age	Age of cached result.

The following example shows the spf cost of each route from router 172.20.168.41:

```
ServiceRouter# show ip ospf rspf route 172.20.168.41

OSPF Process ID p1 context default, Routing Table
  (D) denotes route is directly attached    (R) denotes route is in RIB
192.168.78.0/24 area 0, spf cost 0
192.168.79.0/24 area 0, spf cost 3
192.168.82.0/24 area 0, spf cost 1
193.0.50.0/24 area 0, spf cost 10
193.0.51.0/24 area 0, spf cost 30
```

```
193.0.52.0/24 area 0, spf cost 30
193.0.53.0/24 area 0, spf cost 30
193.0.54.0/24 area 0, spf cost 30
193.0.55.0/24 area 0, spf cost 30
193.0.56.0/24 area 0, spf cost 30
193.0.57.0/24 area 0, spf cost 30
193.0.58.0/24 area 0, spf cost 30
193.0.59.0/24 area 0, spf cost 30
193.0.60.0/24 area 0, spf cost 30

ServiceRouter#
```

Related Commands

Command	Description
router ospf	Enables the OSPF routing process.

show ip ospf traffic

To display OSPF traffic statistics, use the **show ip ospf traffic** command in user EXEC configuration mode.

show ip ospf traffic

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show ip ospf traffic** command:

```
ServiceRouter# show ip ospf traffic

Packet Counter:
 OSPF Process ID p1 context default, Packet Counters (cleared 00:04:33 ago)
  Total: 324 in, 160 out
  LSU transmissions: first 1, rxmit 0, for req 0
  Flooding packets output throttled (IP/tokens): 0 (0/0)
  Ignored LSAs: 0, LSAs dropped during SPF: 0
  LSAs dropped during graceful restart: 0
  Errors: drops in        0, drops out       0, errors in       0,
          errors out      0, hellos in       0, dbds in         0,
          lsreq in        0, lsu in          0, lsacks in       0,
          unknown in      0, unknown out     0, no ospf         0,
          bad version     0, bad crc         0, dup rid         0,
          dup src         0, invalid src     0, invalid dst     0,
          no nbr          0, passive         0, wrong area      0,
          pkt length      0, nbr changed rid/ip addr            0
          bad auth        0

           hellos       dbds     lsreqs       lsus       acks
   In:         84          0          0        118        122
  Out:         31        101          0          1         27

ServiceRouter#
```

Table 2-57 describes the significant fields included in the display above.

Table 2-57 Significant fields included in output of the show ip ospf traffic

Field	Description
Packet Counter	When packet counter last cleared.
Total	Total number of packets in and out from OSPF process.

Table 2-57 Significant fields included in output of the show ip ospf traffic (continued)

Field	Description
Errors	Number of packets have error and dropped because of different reasons.
In	Total count (after last **clear ip ospf traffic**) of the different types of OSPF packets that OSPF process received.
Out	Total count (after last **clear ip ospf traffic**) of the different types of OSPF packets that OSPF process sent.

Related Commands

Command	Description
router ospf	Enables the OSPF routing process.

show ip proximity algorithm

To display the proximity algorithm options currently in use by this Proximity Engine, use the **show ip proximity algorithm** command in user EXEC configuration mode.

show ip proximity algorithm

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

When BGP is configured as the routing protocol, the output from **show ip proximity algorithm** has information on the following:

- Whether the community-based proximity option (location-community) is enabled
- Whether the proximity redirect option is enabled
- Whether the BGP best-path (AS hops) based proximity option is enabled

These threes options are enabled with the **proximity algorithm bgp** command. For information on these options, see the proximity algorithm bgp command.

Examples

The following example shows sample output from the **show ip proximity algorithm** command.

```
ServiceRouter> show ip proximity algorithm

Proximity algorithm: bgp community

ServiceRouter#
```

Related Commands

Command	Description
proximity algorithm bgp	Enables a BGP proximity algorithm option for the Proximity Engine.
proximity engine enable	Enables the Proximity Engine.

show ip proximity servers

To display the interface addresses and hostnames of the Proximity Servers currently in use by this Proximity Engine, use the **show ip proximity servers** command in user EXEC configuration mode.

show ip proximity servers

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command shows other proximity servers and their interface addresses for use in redirection. The DHT ring must be enabled between these proximity servers using the **router srp** command for the DHT ring to be formed. These servers are used for redirection only if the **proximity algorithm bgp redirect** command is enabled.

Examples

The following example shows sample output from the **show ip proximity servers** command.

```
ServiceRouter# show ip proximity servers
Proximity servers:
Hostname: Hostname not found
IP0: 3.1.4.14
IP1: 192.168.82.10
Hostname: Hostname not found
IP0: 3.1.4.12
IP1: 192.168.82.199
Hostname: SN-CDSM
IP0: 192.168.86.77
IP1: 1.100.8.190
ServiceRouter#
```

Related Commands

Command	Description
router srp	Enters SRP configuration mode.
proximity algorithm bgp redirect	Specifies the BGP AS-based redirection on the Proximity Engine.
proximity engine enable	Enables the Proximity Engine.

show ip rib clients

To display details of all the routing protocol instances that are clients of the RIB, use the **show ip rib clients** command in user EXEC configuration mode.

show ip rib clients

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command is used to display detailed information about all routing protocol instances that have registered with RIB.

Examples

The following example shows sample output from the **show ip rib clients** command. The output shows three routing protocol instances that have registered with RIB, along with the results of various counters in RIB.

```
ServiceRouter# show ip rib clients

Displaying information for all clients:CLIENT: direct
 epid: 352       MTS SAP: -1        MRU cache hits/misses:        3/1
 Routing Instances:
  route context "default" table "default"
 Messages received:
  Register          : 1      Add-one-route     : 3      Denotify-request  : 1
 Messages sent:

CLIENT: isis-abc
 epid: 19498     MTS SAP: 1666      MRU cache hits/misses:  1137375/1
 Routing Instances:
  route context “default” table “default”
 Messages received:
  Register          : 1      Add-route         : 52647  Delete-route      : 48872
  Notify-request    : 1
 Messages sent:
  Add-route-ack     : 52647  Delete-route-ack  : 48872

CLIENT: isis-abc-te
 epid: 19498     MTS SAP: 1666      MRU cache hits/misses:        0/0
 Messages received:
  Register          : 1
 Messages sent:
```

Related Commands

Command	Description
proximity engine enable	Enables the Proximity Engine.

show ip rib memory

To display the memory usage information of the RIB, use the **show ip rib memory** command in user EXEC configuration mode.

show ip rib memory

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command is used to display detailed information about the memory usage of the RIB (for example, shared memory information and memory used by routes).

Examples

The following example shows sample output from the **show ip rib memory** command:

```
ServiceRouter# show ip rib memory
Shared memory information for /topos_shm_urib,
Current-Size         HWM    Maximum-Size
     3897168     3897168       131072000
allocated:7   alloc errs:0

URIB slab block statistics:
                  alloc fail   cumm alloc   cumm freed   high-water
urib routes                0            5            0            5
urib nibs                  0            1            0            1
urib rte nibs              0          330          325            5
urib tib nibs              0            1            0            1
urib next hops             0          330          325            5
urib chlst elms            0            5            0            5
urib nhlfes                0            0            0            0
crib nodes                 0            0            0            0
crib routes                0            0            0            0
crib uroutes               0            0            0            0
crib next hops             0            0            0            0

URIB slab statistics:
                   allocated   cumm alloc   cumm freed   high-water
urib routes             8538         8538            0         8538
urib nibs                  2            2            0            2
urib rte nibs           8515       550792       542277         8538
urib tib nibs              2            2            0            2
urib next hops          8515       550792       542277         8538
urib chlst elms         8538         8538            0         8538
urib nhlfes                0            0            0            0
crib nodes                 0            0            0            0
crib routes                0            0            0            0
crib uroutes               0            0            0            0
crib next hops             0            0            0            0
```

Related Commands

Command	Description
proximity engine enable	Enables the Proximity Engine.

show ip rib recursive-next-hop

To display IP recursive next-hop information from the RIB, use the **show ip rib recursive-next-hop** command in user EXEC configuration mode.

show ip rib ip recursive-next-hop [*ip_addr*]

Syntax Description

ip_addr	IP address for which recursive next-hop information is displayed.

Command Defaults

In no *ip_addr* argument is specified, **show ip rib recursive-next-hop** displays information for all recursive next-hops for this Proximity Engine.

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command is used to display IP recursive next-hop information from the RIB.

Examples

The following example shows sample output from the **show ip rib recursive-next-hop** command.

```
ServiceRouter# show ip rib recursive-next-hop

IP Recursive Next-Hop Table

192.168.79.3/32, uptime: 3d22h, bgp-301
192.168.82.1/32, uptime: 3d22h, bgp-301

ServiceRouter> show ip rib recursive-next-hop 192.168.82.1

IP Recursive Next-Hop Table

192.168.82.1/32, uptime: 3d22h, bgp-301

ServiceRouter#
```

In the output, bgp-301 is the number of the BGP Autonomous System containing the recursive next hop.

Related Commands

Command	Description
proximity engine enable	Enables the Proximity Engine.

show ip rib route

To display IP RIB route information, use the **show ip rib route** command in user EXEC configuration mode.

show ip rib route [*ip_address* | **bgp** | **direct** | **isis** | **ospf** | **static** | **summary**]

Syntax Description

ip_address	(Optional) Specifies an IP address for the RIB route.
bgp	(Optional) Specifies the BGP route.
direct	(Optional) Specifies a direct/connected route.
isis	(Optional) Specifies an ISO IS-IS route.
ospf	(Optional) Specifies an OSPF route.
static	(Optional) Specifies static routes.
summary	(Optional) Displays route counts.

Command Defaults

In no *ip_address* argument is specified, **show ip rib route** displays information for all routes for this Proximity Engine.

Command Modes

User EXEC configuration mode.

Examples

The following example shows sample output from the **show ip rib route** command:

```
ServiceRouter# show ip rib route
IP Urib Route Table:
     '*' denotes best ucast next-hop     '**' denotes best mcast next-hop
' [ x/y ] ' denotes [ preference/metric ]

1.1.1.1/32, 1 ucast next-hops, 0 mcast next-hops
    *via 203.0.0.1, GigabitEthernet 2/0, [ 115/20 ] , 04:34:54, isis-p1, L2 2.2.2.2/32, 1
ucast next-hops, 0 mcast next-hops
    *via 203.0.0.1, GigabitEthernet 2/0, [ 115/30 ] , 04:34:54, isis-p1, L2 2.8.1.0/24, 1
ucast next-hops, 0 mcast next-hops, attached
    *via 2.8.1.8, GigabitEthernet 1/0, [ 0/0 ] , 04:35:13, direct 12.0.0.0/8, 1 ucast
next-hops, 0 mcast next-hops
    *via 203.0.0.1, GigabitEthernet 2/0, [ 115/20 ] , 04:34:54, isis-p1, L2 20.0.0.0/16, 1
ucast next-hops, 0 mcast next-hops
    *via 203.0.0.1, GigabitEthernet 2/0, [ 200/0 ] , 04:34:53, bgp-209, internal, tag 209
       extended route information: AS Hops 0, BGP peer AS 209 101.0.0.0/8, 1 ucast
next-hops, 0 mcast next-hops
    *via 203.0.0.1, GigabitEthernet 2/0, [ 200/0 ] , 04:35:03, bgp-209, internal, tag
65209
       extended route information: AS Hops 1, BGP peer AS 209 102.0.0.0/8, 1 ucast
next-hops, 0 mcast next-hops
    *via 203.0.0.1, GigabitEthernet 2/0, [ 200/0 ] , 04:34:53, bgp-209, internal, tag
65209
       extended route information: AS Hops 1, BGP peer AS 209 103.0.0.0/8, 1 ucast
next-hops, 0 mcast next-hops
    *via 203.0.0.1, GigabitEthernet 2/0, [ 200/0 ] , 04:34:53, bgp-209, internal, tag
65209
```

```
       extended route information: AS Hops 1, BGP peer AS 209 201.0.0.0/8, 1 ucast
next-hops, 0 mcast next-hops
    *via 203.0.0.1, GigabitEthernet 2/0, [ 200/0 ] , 04:35:03, bgp-209, internal, tag 209
       extended route information: AS Hops 0, BGP peer AS 209 202.0.0.0/8, 1 ucast
next-hops, 0 mcast next-hops
    *via 203.0.0.1, GigabitEthernet 2/0, [ 200/0 ] , 04:34:53, bgp-209, internal, tag 209
       extended route information: AS Hops 0, BGP peer AS 209 203.0.0.0/8, 1 ucast
next-hops, 0 mcast next-hops, attached
    *via 203.0.0.205, GigabitEthernet 2/0, [ 0/0 ] , 04:35:13, direct 204.0.0.0/8, 1 ucast
next-hops, 0 mcast next-hops
    *via 203.0.0.1, GigabitEthernet 2/0, [ 115/30 ] , 04:34:54, isis-p1, L2 205.0.0.0/8, 1
ucast next-hops, 0 mcast next-hops
    *via 203.0.0.1, GigabitEthernet 2/0, [ 115/20 ] , 04:34:54, isis-p1, L2
ServiceRouter#
```

The following example shows how to display the static route configuration in URIB:

```
ServiceRouter# show ip rib route static
IP Urib Route Table:
    '*' denotes best ucast next-hop     '**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]

10.1.1.0/24, 1 ucast next-hops, 0 mcast next-hops
   *via GigabitEthernet 2/0, [1/0], 00:26:07, static
10.1.2.0/24, 1 ucast next-hops, 0 mcast next-hops
   *via GigabitEthernet 2/0, [1/0], 00:26:07, static
10.1.3.0/24, 1 ucast next-hops, 0 mcast next-hops
   *via GigabitEthernet 2/0, [1/0], 00:26:07, static
10.1.4.0/24, 1 ucast next-hops, 0 mcast next-hops
   *via GigabitEthernet 2/0, [1/0], 00:26:07, static
```

Related Commands

Command	Description
ip rib route	Configures unicast static routes for the Proximity Engine.
proximity engine enable	Enables the Proximity Engine.
show ip static route	Displays IP static route information.

show ip rib unresolved-next-hop

To display unresolved next-hop information from the RIB, use the **show ip rib unresolved-next-hop** command in user EXEC configuration mode.

show ip rib unresolved-next-hop [*ip_address*]

Syntax Description

ip_address	IP address for which recursive next-hop information is displayed.

Command Defaults

In no *ip_address* argument is specified, **show ip rib recursive-next-hop** displays information for all unresolved next-hops for this Proximity Engine.

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command is used to display unresolved next-hop information from the RIB. It is normal to have zero unresolved next-hops. When incoming packets contain a next-hop address that cannot be resolved (that is, cannot be found during the route lookup), the count of unresolved next-hops increases.

Examples

The following example shows sample output from the **show ip rib unresolved-next-hop** command.

```
ServiceRouter# show ip rib unresolved-next-hop

Information about unresolved next-hops for context "default"
Proximity Engine
Number of unresolved nexthops: 0

ServiceRouter#
```

Related Commands

Command	Description
proximity engine enable	Enables the Proximity Engine.

show ip routes

To display the IP routing table, use the **show ip routes** command in EXEC configuration mode.

show ip routes

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **show ip routes** command displays the policy routing tables. The main routing table is always displayed first, and if any policy routing tables have been instantiated, they are also displayed after the main table.

Examples

The **show ip routes** command displays the IP routing table that shows actual routes in the system.

Table 2-58 describes the fields shown in the **show ip routes** display.

Table 2-58 show ip routes Field Descriptions

Field	Description
Destination	Destination address IP route mask.
Gateway	IP address or IP alias of the gateway router.
Netmask	Subnet mask of the gateway router.

The following example shows sample output from the **show ip routes** command:

```
ServiceRouter# sh ip routes
Destination      Gateway          Netmask
---------------- ---------------- ----------------
202.0.0.22       203.0.0.1        255.255.255.255
20.0.40.1        2.8.1.204        255.255.255.255
12.0.0.2         203.0.0.1        255.255.255.255
20.0.60.1        2.8.1.206        255.255.255.255
13.0.0.3         203.0.0.1        255.255.255.255
2.2.2.2          203.0.0.1        255.255.255.255
204.0.0.2        203.0.0.1        255.255.255.255
20.0.50.1        2.8.1.205        255.255.255.255
13.0.0.1         203.0.0.1        255.255.255.255
12.0.0.1         203.0.0.1        255.255.255.255
20.0.10.1        2.8.1.201        255.255.255.255
20.0.70.1        2.8.1.207        255.255.255.255
201.0.0.12       203.0.0.1        255.255.255.255
20.0.30.1        2.8.1.203        255.255.255.255
20.0.20.1        2.8.1.202        255.255.255.255
20.0.80.1        2.8.1.208        255.255.255.255
```

```
2.8.1.0          0.0.0.0          255.255.255.0
20.0.0.0         2.8.1.201        255.0.0.0
172.0.0.0        2.8.1.1          255.0.0.0
10.0.0.0         2.8.1.1          255.0.0.0
203.0.0.0        0.0.0.0          255.0.0.0
0.0.0.0          2.8.1.1          0.0.0.0
```

Related Commands

Command	Description
ip	Changes initial network device configuration settings.

show ip static route

To display IP static route information, use the **show ip static route** command in user EXEC configuration mode.

show ip static route

Syntax Description

This command has no keywords or arguments.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Examples

The following example shows sample output from the **show ip rib route** command:

```
ServiceRouter# show ip static route
IPv4 Unicast Static Routes:
  10.1.1.0/24, configured nh: 0.0.0.0/32
    real nh: 0.0.0.0, iod: 8 [1/0]
  10.1.2.0/24, configured nh: 0.0.0.0/32
    real nh: 0.0.0.0, iod: 8 [1/0]
  10.1.3.0/24, configured nh: 0.0.0.0/32
    real nh: 0.0.0.0, iod: 8 [1/0]
  10.1.4.0/24, configured nh: 0.0.0.0/32
    real nh: 0.0.0.0, iod: 8 [1/0]
  10.1.5.0/24, configured nh: 0.0.0.0/32
    real nh: 0.0.0.0, iod: 8 [1/0]
  10.1.6.0/24, configured nh: 0.0.0.0/32
    real nh: 0.0.0.0, iod: 8 [1/0]
```

Related Commandsl

Command	Description
ip rib route	Configures unicast static routes for the Proximity Engine.
show ip rib route	Displays IP RIB route information.

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 Defaults

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 isis adjacency

To display IS-IS adjacencies, use the **show isis adjacency** command in user EXEC configuration mode.

show isis adjacency [**detail**]

Syntax Description

detail	(Optional) Displays neighbor IP addresses and active topologies.

Command Modes

User EXEC configuration mode.

Command Defaults

By default, this command displays a summarized report on IS-IS adjacency.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show isis adjacency** command with and without the parameter keyword **detail**:

```
ServiceRouter# show isis adjacency detail

IS-IS adjacency database:
System ID       SNPA            Level  State  Hold Time  Interface
0200.c0a8.5401  0000.a1e8.e019  1      UP     00:00:32   GigabitEthernet 3/0
  Up/Down transitions: 3, Last transition: 18:45:08 ago
  Circuit Type: 1-2
  IPv4 Address: 192.168.84.1
  IPv6 Address: 0::
  Circuit ID: 7301-7-core.01, Priority: 64

7301-7-core     001d.a1e9.c41b  1      UP     00:00:08   GigabitEthernet 3/0
  Up/Down transitions: 1, Last transition: 18:45:52 ago
  Circuit Type: 1-2
  IPv4 Address: 192.168.84.7
  IPv6 Address: 0::
  Circuit ID: 7301-7-core.01, Priority: 64

7301-7-core     001d.a1e9.c41b  2      UP     00:00:07   GigabitEthernet 3/0
  Up/Down transitions: 1, Last transition: 18:37:20 ago
  Circuit Type: 1-2
  IPv4 Address: 192.168.84.7
  IPv6 Address: 0::
Circuit ID: 7301-7-core.01, Priority: 64

ServiceRouter#

ServiceRouter# show isis adjacency

IS-IS adjacency database:
System ID       SNPA            Level  State  Hold Time  Interface
0200.c0a8.5401  0000.a1e8.e019  1      UP     00:00:29   GigabitEthernet 3/0
7301-7-core     001d.a1e9.c41b  1      UP     00:00:08   GigabitEthernet 3/0
7301-7-core     001d.a1e9.c41b  2      UP     00:00:10   GigabitEthernet 3/0
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

show isis clns route

To display one or all the destinations to which the router knows how to route CLNS packets, use the **show isis clns route** command in user EXEC configuration mode.

show isis clns route *nsap*

Syntax Description

nsap	CLNS Network Service Access Point (NSAP) address.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

The **show isis clns route** command shows the IS-IS Level 2 routing table and static and Intermediate System-to-Intermediate System Interior Gateway Routing Protocol (ISO-IGRP) learned prefix routes. This table stores IS-IS area addresses and prefix routes. This command requires a Proximity Engine license.

Examples

The following is sample output from the **show clns route** command when the *nsap* argument is not used:

```
ServiceRouter# show isis clns route

IS-IS Level-1 IS routing table
7301-5-Core.00, Instance 0x00000145
   *via 7301-7-core, GigabitEthernet 3/0, metric 20
7301-7-core.00, Instance 0x00000145
   *via 7301-7-core, GigabitEthernet 3/0, metric 10
7301-7-core.02, Instance 0x00000145
   *via 7301-7-core, GigabitEthernet 3/0, metric 20
0200.c0a8.5401.00, Instance 0x00000145
   *via 0200.c0a8.5401, GigabitEthernet 3/0, metric 10
0200.cf00.0002.00, Instance 0x00000145
   *via 0200.c0a8.5401, GigabitEthernet 3/0, metric 20
0200.cf00.0002.01, Instance 0x00000145
   *via 0200.c0a8.5401, GigabitEthernet 3/0, metric 20
0200.cf00.2802.00, Instance 0x00000145
   *via 0200.c0a8.5401, GigabitEthernet 3/0, metric 30
0200.cf00.2802.01, Instance 0x00000145
   *via 0200.c0a8.5401, GigabitEthernet 3/0, metric 30
0200.cf00.5002.00, Instance 0x00000145
   *via 0200.c0a8.5401, GigabitEthernet 3/0, metric 40
0200.cf00.5002.01, Instance 0x00000145
-- More --
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

show isis database

To display the IS-IS link-state database, use the **show isis database** command in user EXEC configuration mode.

show isis database [[*LSP_ID*] [**detail**] | **advertise** | **private** | **summary**]

Syntax Description

LSP_ID	(Optional) LSP ID in the form of xxxx.xxxx.xxxx.xxxx or name.
detail	(Optional) Displays detailed IS-IS information. When specified, the contents of each link-state packet (LSP) are displayed. Otherwise, a summary display is provided.
advertise	(Optional) Displays advertise detail information.
private	(Optional) Displays private information.
summary	(Optional) Displays summary IS-IS information.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

Each option for this command can be entered in an arbitrary string within the same command entry. For example, the following are both valid command specifications and provide the same output: **show isis database detail l2** and **show isis database l2 detail**. This command requires a Proximity Engine license.

Examples

The following is sample output from the **show isis database** command when it is issued with no keywords or arguments:

```
ServiceRouter# show isis database summary

IS-IS LSP database:
IS-IS Level-1 Link State Database
  LSP : 3

IS-IS Level-2 Link State Database
  LSP : 3

ServiceRouter#
```

The following is sample output from the **show isis database** command when it is issued with the **private** keyword:

```
ServiceRouter# show isis database private

IS-IS LSP database:
IS-IS Level-1 Link State Database
  LSPID                 Seq Number   Checksum  Lifetime   A/P/O/T
  DD10-CDE205-2.00-00 * 0x00000004   0x7D13    992        0/0/1/3
    Instance      :  0x00000004
    Digest Offset : 0
    Area Address  :  49.0000
```

```
    NLPID         :  0xCC
    Router ID     :  3.1.5.3
    IP Address    :  3.1.5.3
    Hostname      :  DD10-CDE205-2      Length : 13
    Extended IS   :  DD10-CDE205-2.01   Metric : 10
    Extended IP   :         3.1.5.0/24  Metric : 10          (U)
    Extended IP   :        26.0.0.0/8   Metric : 10          (U)
  DD10-CDE205-2.01-00 * 0x00000001   0x8ABC    992        0/0/0/3
    Instance      :  0x00000001
    Digest Offset : 0
    Extended IS   :  DD10-7301-6.00     Metric : 0
    Extended IS   :  DD10-CDE205-2.00   Metric : 0
  DD10-7301-6.00-00     0x00000003   0x206E    988        0/0/0/3
    Instance      :  0x00000000
    Digest Offset : 0
    Area Address  :  49.0000
    NLPID         :  0xCC
    Hostname      :  DD10-7301-6        Length : 11
    IP Address    :  62.0.0.6
    IP Internal   :        26.0.0.0/8   Metric : 10  (I,U)
    IP Internal   :        62.0.0.0/8   Metric : 10  (I,U)
    IS Neighbor   :  DD10-CDE205-2.01   Metric : 10  (I)
IS-IS Level-2 Link State Database
  LSPID                 Seq Number   Checksum  Lifetime   A/P/O/T
  DD10-CDE205-2.00-00 * 0x00000004   0x7D13    994        0/0/1/3
    Instance      :  0x00000004
    Digest Offset : 0
    Area Address  :  49.0000
    NLPID         :  0xCC
    Router ID     :  3.1.5.3
    IP Address    :  3.1.5.3
    Hostname      :  DD10-CDE205-2      Length : 13
    Extended IS   :  DD10-CDE205-2.01   Metric : 10
    Extended IP   :         3.1.5.0/24  Metric : 10          (U)
    Extended IP   :        26.0.0.0/8   Metric : 10          (U)
  DD10-CDE205-2.01-00 * 0x00000001   0x8ABC    994        0/0/0/3
    Instance      :  0x00000001
    Digest Offset : 0
    Extended IS   :  DD10-7301-6.00     Metric : 0
    Extended IS   :  DD10-CDE205-2.00   Metric : 0
  DD10-7301-6.00-00     0x00000003   0x2668    990        0/0/0/3
    Instance      :  0x00000000
    Digest Offset : 0
    Area Address  :  49.0000
    NLPID         :  0xCC
    Hostname      :  DD10-7301-6        Length : 11
    IP Address    :  62.0.0.6
    IS Neighbor   :  DD10-CDE205-2.01   Metric : 10  (I)
    IP Internal   :        26.0.0.0/8   Metric : 10  (I,U)
    IP Internal   :        62.0.0.0/8   Metric : 10  (I,U)

ServiceRouter#
```

The following is sample output from the **show isis database** command when it is issued with an *LSP_ID* specified:

```
ServiceRouter# sh isis database DD10-CDE205-2.00-00

IS-IS LSP database:
IS-IS Level-1 Link State Database
  LSPID                 Seq Number   Checksum  Lifetime   A/P/O/T
  DD10-CDE205-2.00-00 * 0x00000004   0x7D13    968        0/0/1/3
IS-IS Level-2 Link State Database
  LSPID                 Seq Number   Checksum  Lifetime   A/P/O/T
```

```
  DD10-CDE205-2.00-00 * 0x00000004   0x7D13    970        0/0/1/3

ServiceRouter#
```

The following is sample output from the **show isis database** command when it is issued with the **advertise** keyword:

```
ServiceRouter# show isis database advertise

IS-IS LSP database:
IS-IS Level-1 Link State Database
  LSPID                 Seq Number   Checksum  Lifetime   A/P/O/T
  DD10-CDE205-2.00-00 * 0x00000004   0x7D13    1016       0/0/1/3
    Max: 1446  Used:  104  Free: 1342
    Type:   1, Max:  42, Used:  42, Free:   0
    Type: 129, Max:   1, Used:   1, Free:   0
    Type: 134, Max:   4, Used:   4, Free:   0
      Router ID: 3.1.5.3
    Type:  22, Max: 255, Used:  11, Free: 244
      Extended IS NBR: DD10-CDE205-2.01 (UP)
    Type: 135, Max: 255, Used:  14, Free: 241
      Extended IP Prefix:         3.1.5.0/24  Metric: 10
      Extended IP Prefix:        26.0.0.0/8   Metric: 10
    Type: 137, Max: 255, Used:  13, Free: 242
      Hostname: DD10-CDE205-2  Length: 13
  DD10-CDE205-2.01-00 * 0x00000001   0x8ABC    1016       0/0/0/3
    Max: 1446  Used:   24  Free: 1422
    Type:  22, Max: 255, Used:  22, Free: 233
      Extended IS NBR: DD10-7301-6.00 (UP)
      Extended IS NBR: DD10-CDE205-2.00 (UP)
  DD10-7301-6.00-00     0x00000003   0x206E    1012       0/0/0/3
    Max:    0  Used:    0  Free:    0
IS-IS Level-2 Link State Database
  LSPID                 Seq Number   Checksum  Lifetime   A/P/O/T
  DD10-CDE205-2.00-00 * 0x00000004   0x7D13    1018       0/0/1/3
    Max: 1446  Used:  104  Free: 1342
    Type:   1, Max:  42, Used:  42, Free:   0
    Type: 129, Max:   1, Used:   1, Free:   0
    Type: 134, Max:   4, Used:   4, Free:   0
      Router ID: 3.1.5.3
    Type:  22, Max: 255, Used:  11, Free: 244
      Extended IS NBR: DD10-CDE205-2.01 (UP)
    Type: 135, Max: 255, Used:  14, Free: 241
      Extended IP Prefix:         3.1.5.0/24  Metric: 10
      Extended IP Prefix:        26.0.0.0/8   Metric: 10
    Type: 137, Max: 255, Used:  13, Free: 242
      Hostname: DD10-CDE205-2  Length: 13
  DD10-CDE205-2.01-00 * 0x00000001   0x8ABC    1018       0/0/0/3
    Max: 1446  Used:   24  Free: 1422
    Type:  22, Max: 255, Used:  22, Free: 233
      Extended IS NBR: DD10-7301-6.00 (UP)
      Extended IS NBR: DD10-CDE205-2.00 (UP)
  DD10-7301-6.00-00     0x00000003   0x2668    1014       0/0/0/3
    Max:    0  Used:    0  Free:    0

ServiceRouter#
```

The following is sample output from the **show isis database** command when it is issued with the **detail** keyword:

Note The Proximity Engine becomes a passive listener when the overload bit is present. This is set by default in the LSP originated by the Proximity Engine.

```
ServiceRouter# show isis database detail

IS-IS LSP database:
IS-IS Level-1 Link State Database
  LSPID                 Seq Number   Checksum  Lifetime   A/P/O/T
  DD10-CDE205-2.00-00 * 0x00000004   0x7D13    1007       0/0/1/3
    Area Address  :  49.0000
    NLPID         :  0xCC
    Router ID     :  3.1.5.3
    IP Address    :  3.1.5.3
    Hostname      :  DD10-CDE205-2      Length : 13
    Extended IS   :  DD10-CDE205-2.01   Metric : 10
    Extended IP   :         3.1.5.0/24  Metric : 10          (U)
    Extended IP   :        26.0.0.0/8   Metric : 10          (U)
  DD10-CDE205-2.01-00 * 0x00000001   0x8ABC    1007       0/0/0/3
    Extended IS   :  DD10-7301-6.00     Metric : 0
    Extended IS   :  DD10-CDE205-2.00   Metric : 0
  DD10-7301-6.00-00     0x00000003   0x206E    1002       0/0/0/3
    Area Address  :  49.0000
    NLPID         :  0xCC
    Hostname      :  DD10-7301-6        Length : 11
    IP Address    :  62.0.0.6
    IP Internal   :        26.0.0.0/8   Metric : 10  (I,U)
    IP Internal   :        62.0.0.0/8   Metric : 10  (I,U)
    IS Neighbor   :  DD10-CDE205-2.01   Metric : 10  (I)
IS-IS Level-2 Link State Database
  LSPID                 Seq Number   Checksum  Lifetime   A/P/O/T
  DD10-CDE205-2.00-00 * 0x00000004   0x7D13    1008       0/0/1/3
    Area Address  :  49.0000
    NLPID         :  0xCC
    Router ID     :  3.1.5.3
    IP Address    :  3.1.5.3
    Hostname      :  DD10-CDE205-2      Length : 13
    Extended IS   :  DD10-CDE205-2.01   Metric : 10
    Extended IP   :         3.1.5.0/24  Metric : 10          (U)
    Extended IP   :        26.0.0.0/8   Metric : 10          (U)
  DD10-CDE205-2.01-00 * 0x00000001   0x8ABC    1008       0/0/0/3
    Extended IS   :  DD10-7301-6.00     Metric : 0
    Extended IS   :  DD10-CDE205-2.00   Metric : 0
  DD10-7301-6.00-00     0x00000003   0x2668    1004       0/0/0/3
    Area Address  :  49.0000
    NLPID         :  0xCC
    Hostname      :  DD10-7301-6        Length : 11
    IP Address    :  62.0.0.6
    IS Neighbor   :  DD10-CDE205-2.01   Metric : 10  (I)
    IP Internal   :        26.0.0.0/8   Metric : 10  (I,U)
    IP Internal   :        62.0.0.0/8   Metric : 10  (I,U)
ServiceRouter#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

show isis hostname-table

To display the router-name-to-system-ID mapping table entries for an IS-IS router, use the **show isis hostname-table** command in user EXEC configuration mode.

show isis hostname-table

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

In the IS-IS routing domain, the system ID is used to represent each router. The system ID is part of the network entity title (NET) that is configured for each IS-IS router. For example, a router with a configured NET of 49.0001.0023.0003.000a.00 has a system ID of 0023.0003.000a.
Router-name-to-system-ID mapping is difficult for network administrators to remember during maintenance and troubleshooting on the routers. Entering the **show isis hostname-table** command displays the entries in the router-name-to-system-ID mapping table. This command requires a Proximity Engine license.

Examples

Entering the **show isis hostname-table** command displays the dynamic host mapping table, which displays the router-name-to-system-ID mapping table entries. The * symbol next to the System ID signifies that this is the router-name-to-system-ID mapping information for the local router.

```
ServiceRouter# show isis hostname-table

IS-IS dynamic hostname table:
  Level  System ID       Dynamic hostname
  1      0200.c0a8.0a05  7301-5-Core
  1      0200.c0a8.0a07  7301-7-core
  1      1111.1111.1111* sn-sj83
  2      1234.1234.1234  sn-sj86
  2      1234.1242.1234  7301-2-IS-IS

ServiceRouter#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

show isis interface

To display information about the IS-IS interfaces, use the **show isis interface** command in user EXEC configuration mode.

show isis interface *interface_name*

Syntax Description

interface_name	Interface name.

Command Defaults

Displays all IS-IS interfaces.

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show isis interface** command with interface name set to be GigabitEthernet 1/0 and without an interface name, respectively:

```
ServiceRouter# show isis interface GigabitEthernet 1/0

GigabitEthernet 1/0, Interface status: protocol-down/link-down/admin-down
  IP address: 0.0.0.0, IP subnet: 0.0.0.0/0
  IPv6 routing is disabled
  IS-IS interface operation state : Down/Ready
  Index: 0x0002, Local Circuit ID: 0x02, Circuit Type: 1-2
  Passive level: level-1-2
  LSP interval: 33 ms
  Level      Metric   CSNP  Next CSNP  Hello   Multi   Next IIH
  1              10     10  Never         10   3       Never
  2              10     10  Never         10   3       Never
  Level  Adjs   Ups    Pri  Circuit ID         Since
  1         0     0     64  0000.0000.0000.02  never
  2         0     0     64  0000.0000.0000.02  never

ServiceRouter#

ServiceRouter# show isis interface

GigabitEthernet 1/0, Interface status: protocol-up/link-up/admin-up
  IP address: 172.20.168.83, IP subnet: 172.20.168.0/24
  IPv6 routing is disabled
  Index: 0x0001, Local Circuit ID: 0x01, Circuit Type: 1-2
  Passive level: level-1-2
  LSP interval: 33 ms
  Level      Metric   CSNP  Next CSNP  Hello   Multi   Next IIH
  1              10     10  Never         10   3       Never
  2              10     10  Never         10   3       Never
  Level  Adjs   Ups    Pri  Circuit ID         Since
  1         0     0     64  sn-sj83.01         never
  2         0     0     64  sn-sj83.01         never
```

```
GigabitEthernet 1/0, Interface status: protocol-down/link-down/admin-down
  IP address: 0.0.0.0, IP subnet: 0.0.0.0/0
  IPv6 routing is disabled
  IS-IS interface operation state : Down/Ready
  Index: 0x0002, Local Circuit ID: 0x02, Circuit Type: 1-2
  Passive level: level-1-2
  LSP interval: 33 ms
  Level      Metric   CSNP  Next CSNP  Hello   Multi   Next IIH
  1              10     10  Never         10   3       Never
  2              10     10  Never         10   3       Never
  Level  Adjs   Ups    Pri  Circuit ID         Since
  1         0     0     64  0000.0000.0000.02  never
  2         0     0     64  0000.0000.0000.02  never

GigabitEthernet 2/0, Interface status: protocol-down/link-down/admin-down
  IP address: 0.0.0.0, IP subnet: 0.0.0.0/0
  IPv6 routing is disabled
  IS-IS interface operation state : Down/Ready
  Index: 0x0003, Local Circuit ID: 0x03, Circuit Type: 1-2
  Passive level: level-1-2
  LSP interval: 33 ms
  Level      Metric   CSNP  Next CSNP  Hello   Multi   Next IIH
  1              10     10  Never         10   3       Never
  2              10     10  Never         10   3       Never
  Level  Adjs   Ups    Pri  Circuit ID         Since
  1         0     0     64  0000.0000.0000.03  never
  2         0     0     64  0000.0000.0000.03  never

GigabitEthernet 3/0, Interface status: protocol-up/link-up/admin-up
  IP address: 192.168.84.83, IP subnet: 192.168.84.0/24
  IPv6 routing is disabled
  Index: 0x0004, Local Circuit ID: 0x04, Circuit Type: 1-2
  LSP interval: 33 ms
  Level      Metric   CSNP  Next CSNP  Hello   Multi   Next IIH
  1              10     10  Never         10   3       00:00:08
  2              10     10  Never         10   3       00:00:05
  Level  Adjs   Ups    Pri  Circuit ID         Since
  1         2     2     64  7301-7-core.01     18:55:47
  2         1     1     64  7301-7-core.01     18:47:15

GigabitEthernet 4/0, Interface status: protocol-up/link-up/admin-up
  IP address: 192.168.78.83, IP subnet: 192.168.78.0/24
  IPv6 routing is disabled
  Index: 0x0005, Local Circuit ID: 0x05, Circuit Type: 1-2
  Passive level: level-1-2
  LSP interval: 33 ms
  Level      Metric   CSNP  Next CSNP  Hello   Multi   Next IIH
  1              10     10  Never         10   3       Never
  2              10     10  Never         10   3       Never
  Level  Adjs   Ups    Pri  Circuit ID         Since
  1         0     0     64  sn-sj83.05         never
  2         0     0     64  sn-sj83.05         never

GigabitEthernet 5/0, Interface status: protocol-down/link-down/admin-down
  IP address: 0.0.0.0, IP subnet: 0.0.0.0/0
  IPv6 routing is disabled
  IS-IS interface operation state : Down/Ready
  Index: 0x0006, Local Circuit ID: 0x06, Circuit Type: 1-2
  Passive level: level-1-2
  LSP interval: 33 ms
  Level      Metric   CSNP  Next CSNP  Hello   Multi   Next IIH
  1              10     10  Never         10   3       Never
  2              10     10  Never         10   3       Never
  Level  Adjs   Ups    Pri  Circuit ID         Since
```

```
  1         0     0     64  0000.0000.0000.06  never
  2         0     0     64  0000.0000.0000.06  never

GigabitEthernet 6/0, Interface status: protocol-down/link-down/admin-down
  IP address: 0.0.0.0, IP subnet: 0.0.0.0/0
  IPv6 routing is disabled
  IS-IS interface operation state : Down/Ready
  Index: 0x0007, Local Circuit ID: 0x07, Circuit Type: 1-2
  Passive level: level-1-2
  LSP interval: 33 ms
  Level      Metric   CSNP  Next CSNP  Hello   Multi   Next IIH
  1              10     10  Never         10   3       Never
  2              10     10  Never         10   3       Never
  Level  Adjs   Ups    Pri  Circuit ID         Since
  1         0     0     64  0000.0000.0000.07  never
  2         0     0     64  0000.0000.0000.07  never

GigabitEthernet 7/0, Interface status: protocol-down/link-down/admin-down
  IP address: 0.0.0.0, IP subnet: 0.0.0.0/0
  IPv6 routing is disabled
  IS-IS interface operation state : Down/Ready
  Index: 0x0008, Local Circuit ID: 0x08, Circuit Type: 1-2
  Passive level: level-1-2
  LSP interval: 33 ms
  Level      Metric   CSNP  Next CSNP  Hello   Multi   Next IIH
  1              10     10  Never         10   3       Never
  2              10     10  Never         10   3       Never
  Level  Adjs   Ups    Pri  Circuit ID         Since
  1         0     0     64  0000.0000.0000.08  never
  2         0     0     64  0000.0000.0000.08  never

ServiceRouter#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

show isis ip route

To display the Intermediate IS-IS RSPF route for IS-IS learned routes, use the **show isis ip route** command in user EXEC configuration mode.

show isis ip route [*IP* | **detail** | **summary**]

Syntax Description

IP	(Optional) IP address in the form of *xxx.xxx.xxx.xxx*.
detail	(Optional) Displays detailed IS-IS route information. When specified, the contents of each link-state packet (LSP) are displayed. Otherwise, a summary display for a given IP address is provided.
summary	(Optional) Displays summary IS-IS route information.

Command Defaults

Displays all IS-IS route information.

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show isis route** command with various parameters:

```
ServiceRouter# show isis ip route detail

IS-IS IPv4 routing table

5.5.5.5/32, L2
   *via 192.168.84.7, GigabitEthernet 3/0, metric 20, L2 (I,U)
        Instance 0x0000D831
        LSPID 1234.1242.1234.00-00
12.1.1.1/32, L2
   *via 192.168.84.7, GigabitEthernet 3/0, metric 20, L2 (I,U)
        Instance 0x0000D831
        LSPID 1234.1242.1234.00-00
13.1.1.1/32, L2
   *via 192.168.84.7, GigabitEthernet 3/0, metric 20, L2 (I,U)
        Instance 0x0000D831
        LSPID 1234.1242.1234.00-00
14.1.1.1/32, L2
   *via 192.168.84.7, GigabitEthernet 3/0, metric 20, L2 (I,U)
        Instance 0x0000D831
        LSPID 1234.1242.1234.00-00
22.22.22.22/32, L2
   *via 192.168.84.7, GigabitEthernet 3/0, metric 20, L2 (I,U)
        Instance 0x0000D831
        LSPID 1234.1242.1234.00-00
40.1.1.0/24, L2
   *via 192.168.84.7, GigabitEthernet 3/0, metric 20, L2 (I,U)
 -- More --

ServiceRouter# show isis ip route summary
```

```
IS-IS IPv4 routing table

Total number of best routes  : 8517
Total number of paths        : 12523
Total number of best paths   : 8517
Total number of backup paths : 4006

Best routes per level
  L1         total    : 4006
             direct   : 3
             normal   : 4003
  L2         total    : 4511
             normal   : 4511

Best paths per level
  L1         total    : 4006
             direct   : 3
             normal   : 4003
  L2         total    : 4511
             normal   : 4511

Backup paths per level
  L2         total    : 4006
             direct   : 3
             normal   : 4003

Number of best routes per mask-length
  /24 : 8511    /32 : 6

ServiceRouter#

ServiceRouter# show isis ip route 40.1.1.0

IS-IS IPv4 routing table

40.1.1.0/24, L2
   *via 192.168.84.7, GigabitEthernet 3/0, metric 20, L2 (I,U)

ServiceRouter#

ServiceRouter# show isis ip route 40.1.1.0 detail

IS-IS IPv4 routing table

40.1.1.0/24, L2
   *via 192.168.84.7, GigabitEthernet 3/0, metric 20, L2 (I,U)
        Instance 0x0000D880
        LSPID 1234.1242.1234.00-00

ServiceRouter#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

show isis ip rspf route

To display the Intermediate IS-IS RSPF route for IS-IS learned routes, use the **show isis ip rspf** command in user EXEC configuration mode.

show isis ip rspf route [*LSP_ID*]

Syntax Description

LSP_ID	(Optional) LSP ID in the form of *xxxx.xxxx.xxxx.xxxx* or name.

Command Defaults

If no LSP ID is specified, displays IS-IS RSPF information for all LSP IDs.

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command is used to display the IS-IS RSPF routing information. Output is only displayed for this command when a new proximity request has been received. To clear IS-IS RSPF routing information, use the **clear isis ip rspf route** command. This command requires a Proximity Engine license.

Examples

The following is sample output from the **show isis rspf route** command:

```
ServiceRouter# show isis ip rspf route

LSP ID                 SPF Time  Cache Hit  Level      Age Max range
0200.c0a8.0a01.00-00   01:45:41     0          1       01:43:23 10

ServiceRouter#

ServiceRouter# show isis ip rspf route 0200.c0a8.0a07.00-00

IS-IS IPv4 routing table

172.20.168.0/24, L1
   metric 20, L1
192.168.78.0/24, L1
   metric 20, L1
192.168.79.0/24, L1
   metric 20, L1
192.168.84.0/24, L1
   metric 10, L1
192.168.89.0/24, L1
   metric 10, L1
192.168.90.0/24, L1
   metric 10, L1
207.0.0.0/24, L1
   metric 20, L1
207.0.1.0/24, L1
   metric 30, L1
-- More --

ServiceRouter#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

show isis memory

To display memory usage information for an IS-IS instance, use the **show isis memory** command in user EXEC configuration mode.

show isis memory

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show isis memory** command:

```
ServiceRouter# show isis memory

Shared memory information for /topos-shm-isis-abc,
Current-Size         HWM    Maximum-Size
     2005392     2005392         4194304
IS-IS memory usage:
Type             Size      Count        HWM       Slab   Overhead      Total
Interface        2632          9          9         16      18600      42288
Adjacency         184         35         35         64       5512      11952
LSP DB            320        665        665        704      13136     225936
LSP TLV            48         10         10         64       2768       3248
LSP Retx           72          0          0          0        128        128
Next Hop           24      13130      21970      22528     226736     541856
RT HIX             32          0          0          0        128        128
SPF Adj           104          3          3         64       6520       6832
SPF RT             28      20553      20557      21504      27764     603248
Redist RT          44          3          3       1024      45100      45232
RI                 72          6          6       1024      73472      73904
SPF RT             40          0          1          0        128        128
Redist RT          56          0          0          0        128        128
RI                 56          0          0          0        128        128
Total:                                                    420248    1555136

ServiceRouter#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

show isis process

To display summary information about an IS-IS instance, use the **show isis process** command in user EXEC configuration mode.

show isis process

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show isis process** command:

```
ServiceRouter# show isis process

IS-IS process : abc
  System ID : 1111.1111.1111  IS-Type : L1-L2
  SAP : 1666  Queue Handle : 1666
  Metric-style : advertise(narrow, wide), accept(narrow, wide)
  Area address(es) :
    49.0005
  Process is up and running
  VRF ID: 1
  Stale routes during non-graceful controlled restart
  Interfaces supported by IS-IS :
    GigabitEthernet 0/0
    GigabitEthernet 1/0
    GigabitEthernet 2/0
    GigabitEthernet 3/0
    GigabitEthernet 4/0
    GigabitEthernet 5/0
    GigabitEthernet 6/0
    GigabitEthernet 7/0
  Address family IPv4 unicast :
    Number of interface : 8
    Distance : 115
  Address family IPv6 unicast :
    Number of interface : 0
    Distance : 115
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

show isis rrm

To display IS-IS Received Routing Message (RRM) information, use the **show isis rrm** command in user EXEC configuration mode.

show isis rrm ***int****erface_name*

Syntax Description

interface-name	Interface name

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show isis rrm** command that shows rrm information for all interfaces:

```
ServiceRouter# show isis rrm GigabitEthernet 1/0

IS-IS RRM information for interface GigabitEthernet 1/0:
  No retransmission on non-P2P interface
ServiceRouter# show isis rrm GigabitEthernet 1/0
IS-IS RRM information for interface GigabitEthernet 1/0:
  No retransmission on non-P2P interface

ServiceRouter#

ServiceRouter# show isis rrm GigabitEthernet 2/0

IS-IS RRM information for interface GigabitEthernet 2/0:
  No retransmission on non-P2P interface
ServiceRouter# show isis rrm GigabitEthernet 3/0
IS-IS RRM information for interface GigabitEthernet 3/0:
  No retransmission on non-P2P interface

ServiceRouter#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

show isis spf-log

To display how often and why the router has run a full shortest path first (SPF) calculation, use the **show isis spf-log** command in user EXEC configuration mode.

show isis spf-log [**detail**]

Syntax Description

detail	(Optional) Displays detailed information about the SPF calculation.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from **show isis spf-log** and **show isis spf-log detail** commands, respectively:

```
ServiceRouter# show isis spf-log

IS-IS SPF information:
Total number of SPF calculations: 55836

Log entry (current/max): 20/20
Ago       Level  Reason                                          Count  Total
00:02:49  2      Updated LSP 7301-5-Core.00-0f                       1  0.011510
00:02:49  2      Updated LSP 7301-5-Core.00-10                       1  0.011956
00:02:49  2      Updated LSP 7301-5-Core.00-11                       1  0.011469
00:02:49  2      Updated LSP 7301-5-Core.00-12                       1  0.011503
00:02:49  2      Updated LSP 7301-5-Core.00-13                       1  0.011473
00:02:49  2      Updated LSP 7301-5-Core.00-14                       1  0.011522
00:02:49  2      Updated LSP 7301-5-Core.00-15                       1  0.011514
00:02:49  2      Updated LSP 7301-5-Core.00-16                       1  0.011516
00:02:49  2      Updated LSP 7301-5-Core.00-17                       1  0.011499
00:02:49  2      Updated LSP 7301-5-Core.00-18                       1  0.011530
00:02:49  2      Updated LSP 7301-5-Core.00-19                       1  0.011476
00:02:49  2      Updated LSP 7301-5-Core.00-1a                       1  0.011560
00:02:49  2      Updated LSP 7301-5-Core.00-1b                       1  0.011510
00:02:49  2      Updated LSP 7301-5-Core.00-1c                       1  0.011710
00:02:49  2      Updated LSP 7301-5-Core.00-1d                       1  0.011514
00:02:49  2      Updated LSP 7301-5-Core.00-1e                       1  0.011512
00:02:49  2      Updated LSP 7301-5-Core.00-1f                       1  0.011934
00:02:49  2      Updated LSP 7301-5-Core.00-20                       1  0.011525
00:02:49  2      Updated LSP 7301-5-Core.00-21                       1  0.012232
00:02:49  2      Purged LSP 7301-5-Core.01-00                        1  0.011647

ServiceRouter#

ServiceRouter# show isis spf-log detail

IS-IS SPF information:
```

```
Total number of SPF calculations: 55836

Log entry (current/max): 20/20
Log entry: 01, Ago: 00:03:59, Date: Tue Jan 06 17:34:05 1970
  Level  Instance    Init      SPF       IS Update  URIB Update  Total
  2      0x0000D8C4  0.000019  0.008100  0.000133   0.003255     0.011510
  Level  Node Count   Changed  Reason
  2         8     1         0  Updated LSP 7301-5-Core.00-0f

Log entry: 02, Ago: 00:03:59, Date: Tue Jan 06 17:34:05 1970
  Level  Instance    Init      SPF       IS Update  URIB Update  Total
  2      0x0000D8C5  0.000016  0.008552  0.000129   0.003256     0.011956
  Level  Node Count   Changed  Reason
  2         8     1         0  Updated LSP 7301-5-Core.00-10

Log entry: 03, Ago: 00:03:58, Date: Tue Jan 06 17:34:05 1970
  Level  Instance    Init      SPF       IS Update  URIB Update  Total
  2      0x0000D8C6  0.000016  0.008079  0.000127   0.003243     0.011469
  Level  Node Count   Changed  Reason
  2         8     1         0  Updated LSP 7301-5-Core.00-11

Log entry: 04, Ago: 00:03:58, Date: Tue Jan 06 17:34:05 1970
  Level  Instance    Init      SPF       IS Update  URIB Update  Total
  2      0x0000D8C7  0.000015  0.008097  0.000129   0.003258     0.011503
  Level  Node Count   Changed  Reason
  2         8     1         0  Updated LSP 7301-5-Core.00-12

Log entry: 05, Ago: 00:03:58, Date: Tue Jan 06 17:34:05 1970
  Level  Instance    Init      SPF       IS Update  URIB Update  Total
  2      0x0000D8C8  0.000017  0.008088  0.000129   0.003236     0.011473
  Level  Node Count   Changed  Reason
  2         8     1         0  Updated LSP 7301-5-Core.00-13

Log entry: 06, Ago: 00:03:58, Date: Tue Jan 06 17:34:05 1970
  Level  Instance    Init      SPF       IS Update  URIB Update  Total
  2      0x0000D8C9  0.000019  0.008113  0.000130   0.003257     0.011522
  Level  Node Count   Changed  Reason
  2         8     1         0  Updated LSP 7301-5-Core.00-14

ServiceRouter#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

show isis srm

To display Send Routing Message (SRM) information for an IS-IS, use the **show isis srm** command in privileged EXEC configuration mode.

show isis srm *interface_name*

Syntax Description

interface-name	Interface name.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following example shows how to display sample output from the **show isis srm** command. It shows the srm information on interface GigabitEthernet 1/0:

```
ServiceRouter# show isis srm GigabitEthernet 1/0

IS-IS SRP information for interface GigabitEthernet 1/0:
IS-IS Level-1 Link State Database
Interface is not eligible for flooding LSP
Interface is not on stopped SRM list
LSP interval: 33ms, Next LSP: Never
LSPID                 Seq Number   Checksum  Lifetime   A/P/O/T

IS-IS Level-2 Link State Database
  IS-IS Level-1 Link State Database
Interface is not eligible for flooding LSP
Interface is not on stopped SRM list
LSP interval: 33ms, Next LSP: Never
LSPID                 Seq Number   Checksum  Lifetime   A/P/O/T

ServiceRouter#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

show isis ssn

To display Send Sequence Number (SSN) information for an IS-IS, use the **show isis ssn** command in user EXEC configuration mode.

show isis ssn *interface_name*

Syntax Description

interface-name	Interface name.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show isis ssn** command that shows the ssn information on interface GigabitEthernet 1/0.

```
ServiceRouter# show isis ssn GigabitEthernet 1/0

IS-IS SSN information for interface GigabitEthernet 1/0:
IS-IS Level-1 Link State Database
  Interface is not eligible for sending PSNP
  Next PSNP: Never
  LSPID                 Seq Number   Checksum  Lifetime   A/P/O/T
IS-IS Level-2 Link State Database
  Interface is not eligible for sending PSNP
  Next PSNP: Never
  LSPID                 Seq Number   Checksum  Lifetime   A/P/O/T

ServiceRouter#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

show key chain

To display the key chains in the system, use the **show key chain** command in user EXEC configuration mode.

show key chain [**decrypt** | *name*]

Syntax Description

decrypt	(Optional) Displays key chain information.
name	(Optional) Key chain name.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show key chain** command:

```
ServiceRouter# show key chain
show key chain
Key-Chain lsp
  Key 1 -- text <encrypted-string>
    accept lifetime (00:00:00 Jan 01 1970) - (always valid) [valid now]
    send lifetime (00:00:00 Jan 01 1970) - (always valid) [valid now]

ServiceRouter#
```

Related Commands

Command	Description
key	Creates a key chain and enter into key chain configuration submode.
key chain	Creates a key chain and enter into key chain configuration submode.
key-string	Creates a key string to be used for authentication.

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.

Command 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.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The following is an example of a syslog message for proxy mode native 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 CDS network, you can use the system message log in the CDSM GUI. The CDSM logs only severity level critical or higher messages from registered nodes. Also, the CDSM 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 sysfs partition on the CDSM as /local1/syslog.txt.

The syslog.txt file on the CDSM contains information about events that have occurred on the CDSM 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 CDSM because the problem never occurred on the CDSM 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 movie-streamer

To display the Movie Streamer configuration, use the **show movie-streamer** command in EXEC configuration mode.

show movie-streamer [**bandwidth | cache | proxy**]

Syntax Description

bandwidth	(Optional) Displays Movie Streamer bandwidth configuration.
cache	(Optional) Displays Movie Streamer cache configuration.
proxy	(Optional) Displays Movie Streamer proxy configuration.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows the Movie Streamer configuration:

```
ServiceEngine# show movie-streamer
Movie Streamer version cde220-5.0.3
Movie Streamer is not enabled
------ Movie Streamer General Configurations ------
Movie Streamer max sessions configured: 8000
Movie Streamer transport source ip address is not configured
Movie Streamer accelerate for VOD is enabled
Movie Streamer client idle timeout is 300 seconds
Movie Streamer origin-server idle interval is 10 seconds
Movie Streamer client rtp timeout is 180 seconds
Movie Streamer outgoing bitrate per streamer has no limit
Movie Streamer incoming bitrate per streamer has no limit
------ Movie Streamer Bandwidth Configurations ----
Movie Streamer Outgoing bandwidth enforced is 2000000 kbps
Movie Streamer Incoming bandwidth enforced is 2000000 kbps
------ Movie Streamer Cache Configurations --------
Movie Streamer cache is enabled
Movie Streamer cache age-multiplier: 30%
Movie Streamer cache max-ttl: 1 (days)
Movie Streamer cache revalidate for each request is enabled
------ Movie Streamer Proxy Configurations --------
Movie Streamer proxy has not been configured.
------ Movie Streamer Broadcast List --------------
```

Related Commands

Command	Description
movie-streamer	Enables and configures the Movie Streamer server.
show statistics movie-streamer	Displays statistics for the Movie Streamer.

show multicast

To display the multicast end-user license agreement, use the **show multicast** command in EXEC configuration mode.

show multicast license-agreement

Syntax Description

license-agreement	Displays multicast end-user license agreement.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to display the multicast end-user license agreement:

```
ServiceEngine# show multicast license-agreement

END USER LICENSE

PLEASE READ THE LICENSE AGREEMENT AND ACCEPT BY ENTERING THE FOLLOWING
CLI CONFIGURATION COMMAND: multicast accept-license-agreement

END USER LICENSE AND SOFTWARE WARRANTY
Software License

PLEASE READ THIS SOFTWARE LICENSE CAREFULLY BEFORE DOWNLOADING,
INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE.

<Output Truncated>
```

Related Commands

Command	Description
multicast (Global configuration)	
multicast (EXEC configuration)	

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.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-59 describes the fields shown in the **show ntp status** display.

Table 2-59 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 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.

Command 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 2-60 describes the fields shown in the **show processes** displays.

Table 2-60 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 programs

To display a list of programs on the SE, use the **show programs** command in EXEC configuration mode.

show programs [**movie-streamer** [**cli** | **live** | **rebroadcast**] | **program-id** *id* | **program-name** *name*]

Syntax Description

movie-streamer	(Optional) Displays the list of programs served by the Movie Streamer.
cli	(Optional) Displays the list of CLI programs served by the Movie Streamer.
live	(Optional) Displays the list of live programs served by the Movie Streamer.
rebroadcast	(Optional) Displays the list of rebroadcast programs served by the Movie Streamer.
program-id	(Optional) Displays detailed program information for the specified program ID.
id	Unique number identifying the program.
program-name	(Optional) Displays detailed program information for the specified program name.
name	(Optional) Name of the program.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Typically, users create programs using the CDSM by defining programs in the manifest file or by using the Program API. The **show programs** command output displays the program type, the channel with which the program is associated, the current status of the program, and the next time the program starts and ends.

A program in the Internet Streamer CDS software is defined as a scheduled event in which the content is presented to the end user. Attributes of the program include the start and end time of the program, whether the content is prepositioned or live, the set of SEs assigned to the program, and the streaming server to be used for content delivery.

Program types determine the hardware or software component involved in delivering content to the user. Different program types that are shown in the output of the **show programs** command are as follows:

- Movie streamer live
- Movie streamer rebroadcast

The CDSM GUI allows you to create a program, schedule it, and deliver it over your multicast-enabled CDS network. Programs can consist of prerecorded video or live events. In the case of live events, the Internet Streamer CDS software interoperates with third-party encoders and IP/TV Broadcast Servers to transmit the live stream across the CDS network.

When creating a program in the CDSM GUI, the administrator specifies the following information:

- Streaming server—How the program is streamed or delivered to the end user.
  - Movie Streamer—The event is played from a PC using the Apple QuickTime application or using the IP/TV Viewer application.
  - Exported—The program is exported over HTTP to a set-top box.
- Media source
  - Live stream transmitted from a third-party encoder or an IP/TV Broadcast Server
  - Prepositioned content stored on SEs
- Destination
  - A set of SEs or device groups
  - A channel (live or export)
- Delivery method
  - Unicast or multicast live events
  - Multicast scheduled rebroadcasts
  - TV-out or export playlists
- Schedule
  - Start time and duration
  - Looping forever (enabled or disabled)
  - Multiple playback times
  - Repeating playback times
- Publishing URL—The URL used to view the program

Live Events

Live events are streamed from third-party encoders (such as the Windows Media encoder Version 9 and the QuickTime encoder) or from streaming servers (such as Windows Media Server). The live stream is acquired by the Content Acquirer and transmitted to edge SEs using unicast. From the edge SEs, the live stream is transmitted to end users using either multicast or multicast and unicast live splitting. The live program is available to viewers only during its scheduled times.

Before setting up a live event in the CDSM GUI, the administrator must complete the following tasks:

1. Set up the live event on the encoder or streaming server. This task is done externally to the CDSM GUI.
2. In the CDSM GUI, accept the streaming server's license agreement on the SEs designated to acquire and distribute the stream.
3. Create a live channel (or designate an existing channel as a live channel), assign SEs to the live channel, and designate a Content Acquirer to acquire the stream.

After you have completed the preceding tasks, you are ready to define the program and configure the program settings in the CDSM GUI. The CDSM allows you to define two types of live events based on the streaming server being used:

- WMT live
- Cisco Streaming Engine live

Configuration Requirements for Managed Live Events

If you have channels for live programs configured in your network, make sure that there are no external proxy servers physically located between your Internet Streamer SEs and your Content Acquirer that require proxy authentication. Also, make sure that proxy authentication is not enabled on any receiver SEs that might be in the logical, hierarchical path between the Content Acquirer and the receiver SE that is going to serve the live stream to the requesting clients. If a live stream encounters any device that requires proxy authentication, the stream is dropped before it reaches its destination.

If your network is set up with intermediary devices that require proxy authentication, you can work around the problem by configuring rules to bypass authentication on these devices.

For example, to enable the formation of the unicast splitting tree and, in turn, enable live broadcasting from all receiver SEs, you can specify the following rule on all the parent SEs in the channel:

```
ServiceEngine(config)#  rule pattern-list 1 downstream-SE-ipaddress
ServiceEngine(config)#  rule no-auth pattern-list 1
```

Live Stream Interruptions

During a WMT live broadcast, any interruption of the live stream that lasts 5 minutes or longer causes the multicast broadcast to stop for the duration of the currently scheduled period. If the live stream is interrupted for less than five minutes, the broadcast resumes.

Live stream interruptions can be caused by unexpected encoder failures or by an operational restart. If you have early trials scheduled before the live event, we recommend that you configure multiple schedules, one for each trial. We also recommend that you start the encoder before the scheduled time.

If the live stream stops for more than 5 minutes and resumes later while the program is still scheduled, you can modify the schedule or any other attribute of the program (such as the description) to trigger a restart of the multicast broadcast. Restarting might take up to 5 minutes under these circumstances. This setting does not apply to Movie Streamer live programs.

Scheduled Rebroadcasts

In a scheduled rebroadcast, the prepositioned content is scheduled to be streamed from edge SEs using multicast. To define a program for a rebroadcast event, the administrator must complete the following tasks:

1. Create a content acquisition channel and pre-position the content.
2. Assign media files to the program.
3. Specify the multicast address and port or define a program address pool.
4. Specify the days and times for the rebroadcast.

Note For rebroadcast programs, the media can only be selected from one channel. The SEs and device groups assigned to the channel are selected automatically when you choose the media files for the program.

The CDSM allows you to define a program as a Movie Streamer rebroadcast.

Fast Encoder Failover

The **show programs** command supports encoder failover. The output of the command looks like the following:

Note In the output of the **show programs program-name xxx** command, if the program is a unicast only program, the Priming Status displays.

```
ServiceEngine# show programs program-name live2
Current Time          : May 18 2009 @ 10:10:33 IST      (1242621633)
Program ID            : 1341
Program Name          : live2
Delivery Service ID   : 1340
Delivery Service Name : live2
Type                  : WMT Managed Scheduled Live

Forwarder List        : 3.1.2.11 <- 172.22.28.104

Schedules             :
Schedule # 1:
        Start Time (loc)  : May 18 2009 @ 10:11:00 IST  (1242621660)
        End Time (loc)    : May 18 2009 @ 10:12:00 IST  (1242621720)
        Duration          : 60 secs
        Repeat            : N/A
        Repeatdays        : N/A
        Time spec         : local


Source                :
        Server            : http://172.22.28.104:1881

Destination           :
        Unicast Access URL: rtsp://kinswmt.spcdn.net/live2
        Multicast URL     : http://kinswmt.spcdn.net/live2.nsc.asx
        Multicast Address : 224.2.2.58:94

Start Time (loc)      : May 18 2009 @ 10:11:00 IST      (1242621660)
Start Time            : May 18 2009 @ 04:41:00 GMT      (1242601860)
End Time (loc)        : May 18 2009 @ 10:12:00 IST      (1242621720)
End Time              : May 18 2009 @ 04:42:00 GMT      (1242601920)

Current Status        : Scheduled
Time left             : N/A
Priming Status        :
       Primed            : No
       Current Status    : N/A
       Restarts          : 0

ServiceEngine# show clock
Local time: Mon May 18 10:10:47 IST 2009
RT-612-2# sh programs program-name live2
Current Time          : May 18 2009 @ 10:11:05 IST      (1242621665)
Program ID            : 1341
Program Name          : live2
Delivery Service ID   : 1340
Delivery Service Name : live2
Type                  : WMT Managed Scheduled Live

Forwarder List        : 3.1.2.11 <- 172.22.28.104

Schedules             :
Schedule # 1:
        Start Time (loc)  : May 18 2009 @ 10:11:00 IST  (1242621660)
        End Time (loc)    : May 18 2009 @ 10:12:00 IST  (1242621720)
        Duration          : 60 secs
        Repeat            : N/A
        Repeatdays        : N/A
        Time spec         : local

Source                :
        Server            : http://172.22.28.104:1881
```

```
Destination           :
        Unicast Access URL: rtsp://kinswmt.spcdn.net/live2
        Multicast URL     : http://kinswmt.spcdn.net/live2.nsc.asx
        Multicast Address : 224.2.2.58:94

Start Time (loc)      : May 18 2009 @ 10:11:00 IST      (1242621660)
Start Time            : May 18 2009 @ 04:41:00 GMT      (1242601860)
End Time (loc)        : May 18 2009 @ 10:12:00 IST      (1242621720)
End Time              : May 18 2009 @ 04:42:00 GMT      (1242601920)

Current Status        : Playing
Time left             : 55 secs

ServiceEngine# show clock
Local time: Mon May 18 10:11:10 IST 2009
RT-612-2# sh programs program-name live2
Current Time          : May 18 2009 @ 10:12:10 IST      (1242621730)
Program ID            : 1341
Program Name          : live2
Delivery Service ID   : 1340
Delivery Service Name : live2
Type                  : WMT Managed Scheduled Live

Forwarder List        : 3.1.2.11 <- 172.22.28.104

Schedules             :
Schedule # 1:
        Start Time (loc)  : May 18 2009 @ 10:11:00 IST  (1242621660)
        End Time (loc)    : May 18 2009 @ 10:12:00 IST  (1242621720)
        Duration          : 60 secs
        Repeat            : N/A
        Repeatdays        : N/A
        Time spec         : local

Source                :
        Server            : http://172.22.28.104:1881

Destination           :
        Unicast Access URL: rtsp://kinswmt.spcdn.net/live2
        Multicast URL     : http://kinswmt.spcdn.net/live2.nsc.asx
        Multicast Address : 224.2.2.58:94

Start Time (loc)      : End of Program Reached
Start Time            : End of Program Reached
End Time (loc)        : End of Program Reached
End Time              : End of Program Reached

Current Status        : Stopped
Time left             : N/A

ServiceEngine# show clock
Local time: Mon May 18 10:12:14 IST 2009
```

Now the **show programs** command output contains the forwarder list with the backup source, and the Content Acquirer and non-Content Acquirer output is consistent. Also, if the user executes the **show statistics wmt streamstat** command from the Content Acquirer, the output shows which server is currently serving.

The source URL displays in the source section and the CLI and CDSM are consistent. Because the non-content acquirer cannot get the information on which source is serving, the output contains tips, such as `Please check which source is serving in content acquirer`.

The CDSM parses the backup SDP file and puts the results into the database. The item video_file_back_up saves the backup source server's IP address and port in the play_media table.

Note It is not possible to monitor non-primed streams because they are played directly from the origin server. Primed streams can be monitored because they are buffered on the SE.

Table 2-61 describes the fields shown in the **show programs program-name** and **program-id** display.

Table 2-61 show programs Field Descriptions

Field	Description
Current Time	Date and time of the output.
Program ID	Unique number identifying the program.
Program Name	Name of the program.
Delivery Service ID	Unique number identifying the delivery service.
Delivery Service Name	Unique name identifying the delivery service.
Type	Program type. Program types are as follows: • Movie streamer live • Movie streamer rebroadcast • Windows Media live • Windows Media rebroadcast
Forwarder List	List with primary and backup origin server's IP address.
Schedules	Schedule list. Information is as follows: • Start Time (loc) • End Time (loc) • Duration • Repeat • Repeatdays • Time spec
Source (for Content Acquirer)	Primary and backup source URLs.
Source (for Non-content Acquirer)	Primary and backup source URLs and tips.
Destination	Unicast URLs.

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.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-62 describes the fields shown in the **show radius-server** display.

Table 2-62 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 2-62 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 rcp

To display Remote Copy Program (RCP) information, use the **show rcp** command in EXEC configuration mode.

show rcp

Syntax Description

This command has no keywords or arguments.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to display RCP information:

```
ServiceEngine# show rcp
rcp service configurations:
rcp             enable
```

Related Commands

Command	Description
rcp	Enables the RCP.

show rtsp

To display the Real-Time Streaming Protocol (RTSP) configurations, use the **show rtsp** command in EXEC configuration mode.

show rtsp [**gateway**]

Syntax Description

gateway	(Optional) Displays the RTSP gateway configuration.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example display the output of the **show rtsp gateway** command in EXEC configuration mode:

```
ServiceEngine# show rtsp gateway
RTSP Gateway ip-address 10.107.193.30
RTSP Gateway incoming port 67
RTSP Gateway L4-switch not enabled
RTSP Gateway Transparent Interception:
             Not configured.
```

Related Commands

Command	Description
rtsp	Configure the RTSP-related parameters.

show rule

To display rules configuration information, use the **show rule** command in EXEC configuration mode.

show rule {**action** {**all** [**protocol** {**http** | **rtmp** | **rtsp**}] | **allow** [**protocol** {**http** | **rtmp** | **rtsp**}] | **block** [**protocol** {**http** | **rtmp** | **rtsp**}] | **generate-url-signature** [**protocol** {**http** | **rtmp** | **rtsp**}] | **no-cache** [**protocol** {**http** | **rtmp** | **rtsp**}] | **redirect** [**protocol** {**http** | **rtmp** | **rtsp**}] | **refresh** [**protocol** {**http** | **rtmp** | **rtsp**}] | **rewrite** [**protocol** {**http** | **rtmp** | **rtsp**}] | **validate-url-signature** [**protocol** {**http** | **rtmp** | **rtsp**}]} | **all** | **pattern-list** {*pattern_num* *pattern_type* | **all**}}

Syntax Description

action	Displays all the rules with the same action types.
all	Displays all the action rules.
http	Displays HTTP-related requests for this action.
rtmp	Displays RTMP-related requests for this action.
rtsp	Displays RTSP-related requests for this action.
protocol	(Optional) Specifies the protocol to which actions apply.
allow	Allows the request.
block	Blocks the request.
generate-url-signature	Generates a signed URL.
no-cache	Does not cache the object.
redirect	Redirects the request to the rewritten URL.
refresh	Revalidates the object with the web server.
rewrite	Rewrites the URL and fetch.
validate-url-signature	Validates a signed URL.
all	Displays all the configured actions and pattern lists.
pattern-list	Displays the rules with the specified patterns.
pattern_num	Pattern number. The range is from 1 to 512.
pattern_type	Pattern type (see Table 2-63).
all	Displays rules with all pattern lists.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

You can use the **show rule pattern-list** *pattern_type* command to display rules using a specific pattern type. For a more complete explanation of specific rules, see the "rule" section on page 2-311. Table 2-63 shows the permitted pattern types and describes each pattern type.

Note The **rule action redirect** command does not display the pattern-list header field.

Table 2-63 Pattern Types

Pattern Type	Description
all	Displays configured patterns for all pattern types.
domain	Regular expression to match the domain name.
dst-ip	Destination IP address of the request.
header-field	Request header field pattern.
src-ip	Source IP address of the request.
url-regex	Regular expression to be matched against the URL.
url-regsub	Regular expression to match URL and replacement pattern.

Examples

The following example shows how to display all rules with the configured action types and pattern lists:

```
ServiceEngine# show rule all
Rules Template Configuration
----------------------------
Rule Processing Enabled
rule block domain bar.com
rule block domain \.foo.com
rule rewrite url-regsub http://www.ietf.org/rfc/.* http://wwwin-eng.cisco.com/RFC/$1
rule no-cache dst-ip 172.31.120.0 255.255.192.0
rule no-cache url-regex \.*cgi-bin*
```

Related Commands

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.
rule	Sets the rules by which the SE filters HTTP, HTTPS, and RTSP traffic.

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 keywords or arguments.

Command 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
! CDS 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
!
!
!
!
!
movie-streamer enable
movie-streamer max-concurrent-sessions 10000
movie-streamer advanced client idle-timeout 0
movie-streamer advanced client rtp-timeout 0
bitrate movie-streamer outgoing 6000000
bitrate movie-streamer incoming 6000000
!
rtsp advanced max-request-rate 1000
wmt max-concurrent-sessions 14000
wmt cache min-ttl 1
wmt cache max-ttl days 3
wmt advanced client idle-timeout 300
wmt advanced server inactivity-timeout 300
wmt transaction-logs format extended wms-90
!
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
!
!
```

```
aaa authentication login local secondary
aaa authentication login tacacs+ primary
aaa authorization exec local secondary
aaa authorization exec tacacs+ primary
!
ftp enable
!
telnet enable
!
!
!
!
!
!
!
cdsm 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
!
bandwidth wmt outgoing 6000000 default
bandwidth wmt outgoing 6000000 max-bandwidth
bandwidth wmt incoming 6000000 default
bandwidth wmt incoming 6000000 max-bandwidth
bandwidth movie-streamer outgoing 6000000 default
bandwidth movie-streamer outgoing 6000000 max-bandwidth
bandwidth movie-streamer incoming 6000000 default
bandwidth movie-streamer incoming 6000000 max-bandwidth
!
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 CDS 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 {**access-policy** | **content-based-routing** | **forwarding** [**content-origin** *content_origin*] | **lastresort** [**domain** *name*] | **load** {**all** | **sename** *sename*} | **location-based-routing** | **memory** | **proximity-based-routing** {**cache ip** *ip_address*} | **redirect-burst-control** | **redirect-mode** | **routes** [**content-origin** *content_origin* **ip-address** *ip_address*] | **service-monitor** | **services** {**all** | **sename** *se_name*} | **subscribe domain** | **summary** [**content-origin** *content_origin*]}

On the CDSM:

show service-router service-monitor

Syntax Description

access-policy	Configures the service-router access-policy.
content-based-routing	Displays the content-based routing configuration.
forwarding	Displays the content origin forwarding tables.
content-origin	(Optional) Displays information for one content origin.
content_origin	Content origin FQDN[1].
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.
location-based-routing	Displays the location-based routing configurations.
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.
redirect-mode	Displays the redirect-mode configurations.
routes	Displays the content origin routing tables.

service-monitor	Displays the service monitor configuration.
services	Displays the services status.
subscribe	Displays the subscribe list.
domain	Displays the domain names.
summary	Displays the content origin routing table summary statistics.
keepalive-interval	Displays the keepalive interval.

1. FQDN = fully qualified domain name

Command Defaults

content-based-routing: disabled

Command Modes

EXEC configuration mode.

Usage Guidelines

This command allows users to check the Service Router-releated configuration. Through this command, users can view the configured features of an SR, such as location-based routing and content-based routing.

The **show service-router content-based-routing** command displays the content aware routing configuration for every content-origin. This command displays whether the universal content based routing is enabled or disabled, the content redundant copy number, and whether the content based routing has been disabled for any particular domain.

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 content aware routing configuration for every content-origin:

```
ServiceRouter# show service-router content-based-routing
Content based routing is enabled globally
Content redundant copy 1
Content based routing is disabled for vod.cds.com
Content based routing is disabled for kse.mem
Content based routing is disabled for kse.vod.cds.com
```

The following example shows how to display the proximity routing information on an SR:

```
ServiceRouter# sh service-router proximity-based-routing
Proximity based routing is enabled
Proximity cache timeout 600 seconds
service-router proximity-based-routing proximity-server 127.0.0.1
```

The following example shows how to display the proximity routing cache information on an SR:

```
ServiceRouter# show service-router proximity-based-routing cache ip 171.XX.XXX.XXX

----- Proximity cache information for 171.XX.XXX.XXX -----
Cached proximity information on Fri Jul 30 05:19:50 2010

   SE Name: XX-CDE220-Fiber
   Rating : 3758096385

   SE Name: XX-CDE250-CE-2
   Rating : 3758096385

   SE Name: XXXX-SR
   Rating : 3758096385

   SE Name: XXX-CDE220-1
   Rating : 3758096385

   SE Name: XXX-CDE250-2
   Rating : 3758096385

   SE Name: XX-CDE420-1
   Rating : 3758096385

   SE Name: XXX-CDE420-1
   Rating : 3758096385
```

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,WMT,FMS,WEB,MS,DISK,NIC

Threshold values configured:
----------------------------
CPU         : 80%
MEM         : 80%
```

```
KMEM        : 50%
WMT         : 90%
FMS         : 90%
MS          : 90%
NIC         : 90%
BURST COUNT : 1
DISK        : 80%
DISKFAILCNT : 1

Sample periods configured:
--------------------------
CPU  : 1 (secs)
MEM  : 1 (secs)
KMEM : 1 (secs)
WMT  : 1 (secs)
FMS  : 1 (secs)
NIC  : 3 (secs)
DISK : 1 (secs)

Sample counts configured to use in calculating average:
-------------------------------------------------------
CPU  : 2
MEM  : 2
KMEM : 2
WMT  : 2
FMS  : 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

WMT
Enabled               : Yes
Current Stream Count  : 0
Threshold             : Not reached
Stopped               : No

MS
Enabled               : No

FMS
Enabled               : No
```

The following example shows how to display the Service Router information on the CDSM:

```
CDSM# 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%

CDSM#
```

The following example shows how to display the domains to which the SR is subscribed:

```
ServiceRouter# show service-router subscribe domain
Domains subscribed:
    test1.com
    test5.com
    test4.com
    test3.com
```

Related Commands

Command	Description
service-router	Configures service routing.
clear service-router	Clears the proximity-based routing proximity 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.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to display the services information by the port number:

```
CDSM# 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:

```
CDSM# show services summary

             Service        Ports
-----------------------------------------------------
                 CMS         15256  2000  2001  2002  2003  2004  2005
                 GUI          8001
                 Wmt          1755  1756  1757  1799
                 icp          3128
                emdb          5432
             CertMgr          6001
           MgmtAgent          5252
          Real_Proxy          1090  8082  9002   555 28000  7879  6060  7071  30
31
          Cdsm_UI_http          8443
          Real_Server          7070  8081  9091 27999  7878  7802  1554  3030  40
40  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.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

This command provides information on various SNMP variables and statistics on SNMP operations.

Table 2-64 describes the fields shown in the **snmp alarm-history** display.

Table 2-64 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 CDS device contain numeric alarm IDs.
ModuleID	Traps sent by a CDS device contain numeric module IDs. See Table 2-65 to map module names to module IDs.
Category	Traps sent by an CDS device contain numeric category IDs. See Table 2-66 to map category names to category IDs.
Descr	Description of the Internet Streamer CDS software alarm and the application that generated the alarm.

Table 2-65 describes the mapping of module names to module IDs.

Table 2-65 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 2-66 describes the mapping of category names to category IDs.

Table 2-66 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 2-67 describes the fields shown in the **show snmp stats** display.

Table 2-67 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 2-67 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 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 2-68 describes the fields shown in the **show snmp engineID** display.

Table 2-68 show snmp engineID Field Descriptions

Field	Description
Local SNMP Engine ID	String that identifies the copy of SNMP on the local device.

Table 2-69 describes the fields shown in the **show snmp group** display.

Table 2-69 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 2-70 describes the fields shown in the **show snmp user** display.

Table 2-70 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[1].
snmp-server contact	Sets the system server contact (sysContact) string.
snmp-server enable traps	Enables the 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.

1. SNMP = Simple Network Management Protocol

show srp database

To display the descriptor-related information saved in the descriptor database, use the **show srp database** command in privileged EXEC configuration mode.

show srp database [*key* | **active** | **brief** | **content** | **expired** | **group** | **statistics** | **maincontent** *target_string* | **record** *key target_string* | **service** | **size** *low high* | **subid** *key target_string* | **update** *start end*]

Syntax Description

key	(Optional) DHT key in hexadecimal format that identifies a descriptor to be fetched from the descriptor database,
active	(Optional) Displays the database active entries.
brief	(Optional) Displays brief information for each descriptor in the database, including DHT key, Type, Entity Type, Size, and initial part of the Element Data in Element 0 of the descriptor.
content	(Optional) Filters the descriptor database to display content-type descriptors only.
expired	(Optional) Displays the database expired entries.
group	(Optional) Filters the descriptor database to display group-type (multicast group) descriptors only.
maincontent *target_string*	(Optional) Filters the descriptor database to display descriptors whose Element data field in the main element (Element 0) contains *target_string*.
record *key target_string*	(Optional) In a given descriptor identified by *key*, finds elements whose resource record contains *target_string*.
service	(Optional) Filters the descriptor database to display service-type descriptors only.
size *low high*	(Optional) Filters the descriptor database to display descriptors whose size (in bytes) is no larger than *high* and no smaller than *low*.
statistics	(Optional) Displays the total number of entries in the database.
subid *key target_string*	(Optional) In a given descriptor identified by *key*, finds elements whose sub ID (Element ID) contains the *target_string*.
update *start end*	(Optional) Filters the descriptor database to display descriptors that were updated no earlier than *start* and no later than *end*. Format for *start* and *end* is: *month_date_hour*:*minute*:*second_year*. For example: Sep_8_08:54:55_2007.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command displays information saved in the descriptor database and filters the data based on the argument that is specified. Without specifying any key or argument, it displays a summary of the descriptor database, which contains the DHT key and size for each descriptor and the total number of active descriptors in the database.

By providing the DHT key in hexadecimal format or various filtering arguments, **show srp database** filters through the descriptor database or a particular descriptor to obtain the desired information. Keys with less than 64 hexadecimal characters are appended with zeroes.

In filtering arguments that have a target string, the specified string is case sensitive.

Examples

The following examples show the output **show srp database** displays with and without a DHT key and the optional filtering arguments that specify how to query the database to obtain desired information. All the examples are based on querying the same descriptor database.

The following example is sample output from the **show srp database** command when it is issued with no keywords or arguments.

```
ServiceRouter# show srp database

DHT KEY                                                                : SIZE
0a1405495f14dfc1d6fd10b93d957903456166d3b7b883b9047fb89cbecb5157: 1054
12300000000000000000000000000000000000000000000000000000000000000000: DELETED
15136e3cfb5c3de3c4258d5c16c1bbabc5ddb538b51b32bdc1ebbd9bcb75b6d7: 838
23400000000000000000000000000000000000000000000000000000000000000000: 168
3392b8bfe67c12c326aa346bdff1e83ac6286e397ce0013f8c4a33fc4dc5abda: 1065
352a5e7e0e3dd9b78ab18fdb4408191f8418439b3ffef79f9b0698b8a73c16bc: 853
39da9f8b45b6a186fdfdb6eec44ab71e7510c1de7b1b049df7c971696cb398a0: 1074
4e346a0c197a6e1e69650badd1687557dc4d9b80789407a9b452eda761f1056e: 1056
4f9400b0372d934d5819f3e88f4ad5be2177e96b79ee34aca49722e2db9ff300: 1102
77700000000000000000000000000000000000000000000000000000000000000000: 129
78900000000000000000000000000000000000000000000000000000000000000000: 109
88800000000000000000000000000000000000000000000000000000000000000000: 167
8d3e7478a3685decd322f891ea5a09a6b264097ab166d5b7bedd5ad9715f1401: 1048
99900000000000000000000000000000000000000000000000000000000000000000: 183
a6c4ef5b73c5b5621567946e7691b3d1123f9a3cf8b28ce29a075bfa41cb21ad: 1068
c1898f9a8b69c3912f0fe8fecac30818fab24385fa8a1d37a8ffd193cf3eeebc: 324
c53126d4113799d7f300c6accf526423756efa5e007fc3cc16fe45a9c8c06ee3: 881
ca1329d38687cdd5f8ab7aabe4333ee7883a6a28f7e8b03e11d58bb3f4c39988: 1057
cbb037edbe196fbf8d0f5bfa6e629ff1242483f5f5450719748189cf9d7b1fa4: 1086
e50dc5cca2b736d00c41506b754c7bd331ab38826a4df396f6343a81e5631832: 843
e8ca53dbcf748505194a10c9b6fa1549f309345f19b4d4df920be79d5e986471: 1083
f47ec4f84068b9fda926f4767d2219f4faeabbbb0738312f70917504a0c8c9b9: 863

Total                         21 active item(s) in the database

ServiceRouter#
```

The preceding example shows that there are 22 entries in the database, of which 21 are active ones. If a descriptor is active (has not been deleted), then its size is displayed. Otherwise, DELETED is displayed in the SIZE field of the descriptor. If the descriptor database is empty, the following output is displayed:

```
ServiceRouter# show srp database

DHT   KEY                                                        : SIZE
Total                                  0 active item(s) in the database

ServiceRouter#
```

The following is sample output from the **show srp database** *key* command where the DHT key is 234:

```
ServiceRouter# show srp database 234

Getting database entry for
234

Entity key:
234000000000000000000000000000000000000000000000000000000000000000
Entity rec type:          101     Entity total length: 168
Entity type:         5783093e     Entity flags:        0
--------------- Element 0        (main)-----------------
Element ID: main
  Element total len          45   ID len:      0
  Delete Time: 47af31d505d8fb77
  Flags  8
  Last Update: Sun Feb 10 17:18:34 2008 (47af31ea077ac2e7)
  Expiration : Tue Mar 11 17:18:34 2008 (47d6beea077a0000)
  Element data len:           5
  Element data:
test
--------------- Element 1        (comp)-----------------
Element ID: "123"(313233)
  Element total len          51   ID len:      3
  Last Update: Sun Feb 10 17:24:40 2008 (47af335826c5288f)
  Expiration : Sun Feb 10 17:29:40 2008 (47af348426c50000)
  Element data len:           8
  Element data:

testing

ServiceRouter#
```

In the preceding example, the output is detailed information saved for the descriptor 234:

- Descriptor 234 has a record type 101.
- Its entity type is 5783093e, which means this descriptor (234) is a service-type descriptor.
- Its total length is 168 bytes.
- It has zero Entity flags. Entity flags are not currently used.
- It has two elements:
  - Element ID main is for the descriptor itself. The descriptor's name is test.
  - Element ID 123 is for a resource (testing) that has been added to the descriptor.

The following is sample output from **show srp database** *key* command where the DHT key is 123. In this example, the entity specified by the key has been deleted.:

```
ServiceRouter# show srp database 123

Getting database entry for
123
Entity key:
123000000000000000000000000000000000000000000000000000000000000000
Entity was DELETED on (47b1fabdd076fba7) Tue Feb 12 19:59:57 2008

ServiceRouter#
```

The following is abbreviated sample output from the **show srp database** command when it is issued with the optional argument **brief**:

```
ServiceRouter# show srp database brief

Key: 0a1405495f14dfc1d6fd10b93d957903456166d3b7b883b9047fb89cbecb5157
 Type: Regular  Entity Type: Service     Size:     1054
 Body: <Service xmlns="urn:topos:descriptor:xml
Key: 0a1405495f14dfc1d6fd10b93d957903456166d3b7b883b9047fb89cbecb5157
 Type: Regular  Entity Type: Service     Size:     1054
 Body: <Service xmlns="urn:topos:descriptor:xml

... Output omitted

Key: 77700000000000000000000000000000000000000000000000000000000000000000
 Type: Mcast Cmd        Entity Type: Group       Size:      129
 Body: ..................test.
Key: 78900000000000000000000000000000000000000000000000000000000000000000
 Type: Regular  Entity Type: Group       Size:      109
 Body: test.
Key: 88800000000000000000000000000000000000000000000000000000000000000000
 Type: Regular  Entity Type: Unknown(0)  Size:      167
 Body: test

... Output omitted

Total                        21 active item(s) in the database

ServiceRouter#
```

In the preceding example, **show srp database brief** displays brief information for each descriptor in the database, including DHT key, Type, Entity Type, Size, and Body (the initial part of the Element Data in Element 0 of the descriptor). The Body contains different information, depending on the type of the descriptor displayed.

- By default, Body contains the first 40 printable characters of the main element data.
- If the descriptor is a service type descriptor, Body contains the service name information.

The following is sample output from the **show srp database** command when it is issued with the filtering argument **content**. There are no content-type descriptors in the database:

```
ServiceRouter# show srp database content

Total      0 content type descriptor(s) in the database

ServiceRouter#
```

The following is sample output from the **show srp database** command when it is issued with the filtering argument **service**. There are 16 service-type descriptors in the database:

```
ServiceRouter# show srp database service

0a1405495f14dfc1d6fd10b93d957903456166d3b7b883b9047fb89cbecb5157: Size: 1054
15136e3cfb5c3de3c4258d5c16c1bbabc5ddb538b51b32bdc1ebbd9bcb75b6d7: Size: 838
23400000000000000000000000000000000000000000000000000000000000000000: Size: 168
3392b8bfe67c12c326aa346bdff1e83ac6286e397ce0013f8c4a33fc4dc5abda: Size: 1065
352a5e7e0e3dd9b78ab18fdb4408191f8418439b3ffef79f9b0698b8a73c16bc: Size: 853
39da9f8b45b6a186fdfdb6eec44ab71e7510c1de7b1b049df7c971696cb398a0: Size: 1074
4e346a0c197a6e1e69650badd1687557dc4d9b80789407a9b452eda761f1056e: Size: 1056
4f9400b0372d934d5819f3e88f4ad5be2177e96b79ee34aca49722e2db9ff300: Size: 1102
8d3e7478a3685decd322f891ea5a09a6b264097ab166d5b7bedd5ad9715f1401: Size: 1048
a6c4ef5b73c5b5621567946e7691b3d1123f9a3cf8b28ce29a075bfa41cb21ad: Size: 1068
c53126d4113799d7f300c6accf526423756efa5e007fc3cc16fe45a9c8c06ee3: Size: 881
```

```
ca1329d38687cdd5f8ab7aabe4333ee7883a6a28f7e8b03e11d58bb3f4c39988: Size: 1057
cbb037edbe196fbf8d0f5bfa6e629ff1242483f5f5450719748189cf9d7b1fa4: Size: 1086
e50dc5cca2b736d00c41506b754c7bd331ab38826a4df396f6343a81e5631832: Size: 843
e8ca53dbcf748505194a10c9b6fa1549f309345f19b4d4df920be79d5e986471: Size: 1083
f47ec4f84068b9fda926f4767d2219f4faeabbbb0738312f70917504a0c8c9b9: Size: 863
 Total     16 service type descriptor(s) in the database

ServiceRouter#
```

The following is sample output from the **show srp database** command when it is issued with the filtering argument **group**. There are three group-type descriptors in the database:

```
ServiceRouter# show srp database group

77700000000000000000000000000000000000000000000000000000000000000000: Size: 393
99900000000000000000000000000000000000000000000000000000000000000000: Size: 307
c1898f9a8b69c3912f0fe8fecac30818fab24385fa8a1d37a8ffd193cf3eeebc: Size: 124
 Total      3 group type descriptor(s) in the database

ServiceRouter#
```

The following is sample output from the **show srp database** command when it is issued with the option **statistics**. The output indicates how many descriptors (including deleted ones) exist in the descriptor database:

```
ServiceRouter# show srp database statistics

  Total number of descriptors = 22

ServiceRouter#
```

The following is sample output from the **show srp database** command when it is issued with the filtering argument **maincontent** and the target string **service**. The sample output indicates that there are 15 descriptors in the database whose main content (that is, the Element Data field of Element 0) contains the target string service:

```
ServiceRouter# show srp database maincontent service

0a1405495f14dfc1d6fd10b93d957903456166d3b7b883b9047fb89cbecb5157: Type: 101
  Rec Type: 5783093e Size: 1054
15136e3cfb5c3de3c4258d5c16c1bbabc5ddb538b51b32bdc1ebbd9bcb75b6d7: Type: 101
  Rec Type: 5783093e Size: 838
3392b8bfe67c12c326aa346bdff1e83ac6286e397ce0013f8c4a33fc4dc5abda: Type: 101
  Rec Type: 5783093e Size: 1065
352a5e7e0e3dd9b78ab18fdb4408191f8418439b3ffef79f9b0698b8a73c16bc: Type: 101
  Rec Type: 5783093e Size: 853
39da9f8b45b6a186fdfdb6eec44ab71e7510c1de7b1b049df7c971696cb398a0: Type: 101
  Rec Type: 5783093e Size: 1074
4e346a0c197a6e1e69650badd1687557dc4d9b80789407a9b452eda761f1056e: Type: 101
  Rec Type: 5783093e Size: 1056
4f9400b0372d934d5819f3e88f4ad5be2177e96b79ee34aca49722e2db9ff300: Type: 101
  Rec Type: 5783093e Size: 1102
8d3e7478a3685decd322f891ea5a09a6b264097ab166d5b7bedd5ad9715f1401: Type: 101
  Rec Type: 5783093e Size: 1048
a6c4ef5b73c5b5621567946e7691b3d1123f9a3cf8b28ce29a075bfa41cb21ad: Type: 101
  Rec Type: 5783093e Size: 1068
c53126d4113799d7f300c6accf526423756efa5e007fc3cc16fe45a9c8c06ee3: Type: 101
  Rec Type: 5783093e Size: 881
ca1329d38687cdd5f8ab7aabe4333ee7883a6a28f7e8b03e11d58bb3f4c39988: Type: 101
  Rec Type: 5783093e Size: 1057
cbb037edbe196fbf8d0f5bfa6e629ff1242483f5f5450719748189cf9d7b1fa4: Type: 101
  Rec Type: 5783093e Size: 1086
e50dc5cca2b736d00c41506b754c7bd331ab38826a4df396f6343a81e5631832: Type: 101
```

```
  Rec Type: 5783093e Size: 843
e8ca53dbcf748505194a10c9b6fa1549f309345f19b4d4df920be79d5e986471: Type: 101
  Rec Type: 5783093e Size: 1083
f47ec4f84068b9fda926f4767d2219f4faeabbbb0738312f70917504a0c8c9b9: Type: 101
  Rec Type: 5783093e Size: 863

Total 15 item(s) in the database whose main content contains
'service'

ServiceRouter#
```

The following is sample output from the **show srp database** command when it is issued with the filtering argument **record** to search in a descriptor specified by the key 999 to locate records containing the target string **test**. The examples are in the following order:

- Descriptor for a record where the target string is found.
- Descriptor for a record where the entity has been deleted.
- Descriptor for a record where the target string is not found.

```
ServiceRouter# show srp database record 999 test

Entity key:
999000000000000000000000000000000000000000000000000000000000000000000000
Entity rec type:          101     Entity total length: 183
Entity type:         22222222     Entity flags:        0
--------------- Element 1        (comp)-------4----------
Element ID: "123"(313233)
  Element total len          47   ID len:      3
  Last Update: Tue Feb 12 02:07:38 2008 (47b0ff6ae5e0497b)
  Expiration : Thu Mar 13 02:07:38 2008 (47d88c6ae5e00000)
  Element data len:           4
  Element data:
test

ServiceRouter# show srp database record 123 test
Entity key:
123000000000000000000000000000000000000000000000000000000000000000000000
Entity was DELETED on (47b1fabdd076fba7) Tue Feb 12 19:59:57 2008

ServiceRouter# show srp database record 777 test
Entity key:
777000000000000000000000000000000000000000000000000000000000000000000000
Entity rec type:          102     Entity total length: 129
Entity type:         22222222     Entity flags:        0
There is no resource record containing test

ServiceRouter#
```

The following is sample output from the **show srp database** command when it is issued with the filtering argument **size** to select descriptors whose size is in the given range. This example shows that, for the active descriptors, there are five descriptors whose size is larger than 100 bytes and smaller than 300 bytes:

```
ServiceRouter# show srp database size 100 300

234000000000000000000000000000000000000000000000000000000000000000000000: Type: 101
  Rec Type: 5783093e Size: 168
777000000000000000000000000000000000000000000000000000000000000000000000: Type: 102
  Rec Type: 22222222 Size: 129
789000000000000000000000000000000000000000000000000000000000000000000000: Type: 101
  Rec Type: 22222222 Size: 109
888000000000000000000000000000000000000000000000000000000000000000000000: Type: 101
```

```
  Rec Type:        0 Size: 167
999000000000000000000000000000000000000000000000000000000000000000000000: Type: 101
  Rec Type: 22222222 Size: 183

Total     5 item(s) in the database whose size is between 100 and 300

ServiceRouter#
```

The following example is sample output from the **show srp database** command when it is issued with the filtering argument **subid** to search for elements in a given descriptor whose Element ID contains the given target string. In this example, the search is in the descriptor whose key is 999 and for elements whose sub ID (Element ID) is 123. The output indicates one element, Element 1, with the specified Element ID 123.

```
ServiceRouter# show srp database subid 999 123

Entity key:
999000000000000000000000000000000000000000000000000000000000000000000000
Entity rec type:          101     Entity total length: 183
Entity type:         22222222     Entity flags:        0
--------------- Element 1        (comp)-----------------
Element ID: "123"(313233)
  Element total len          47   ID len:      3
  Last Update: Tue Feb 12 02:07:38 2008 (47b0ff6ae5e0497b)
  Expiration : Thu Mar 13 02:07:38 2008 (47d88c6ae5e00000)
  Element data len:           4
  Element data:
test

ServiceRouter#
```

The following example is sample output from the **show srp database** command when it is issued with the filtering argument **update** to select descriptors that have been updated in the specified time range. The command uses the Last Update field of Element 0 to determine when the descriptor has been updated. The sample output indicates that four descriptors have been updated in the specific time range.

```
ServiceRouter# show srp database update Feb_11_02:07:38_2008 Feb_12_02:07:38_2009

777000000000000000000000000000000000000000000000000000000000000000000000: Type: 102
  Rec Type: 22222222 Size: 129
888000000000000000000000000000000000000000000000000000000000000000000000: Type: 101
  Rec Type:        0 Size: 167
999000000000000000000000000000000000000000000000000000000000000000000000: Type: 101
  Rec Type: 22222222 Size: 183
c1898f9a8b69c3912f0fe8fecac30818fab24385fa8a1d37a8ffd193cf3eeebc: Type: 102
  Rec Type: 22222222 Size: 324

Total 4 active item(s) in the database updated in the specified time duration

ServiceRouter#
```

Related Commands

Command	Description
clear srp descriptor	Deletes a single descriptor or all descriptors in the descriptor database.
show srp multicast database	Displays multicast database information for an SRP process

show srp leafset

To display SRP leafset information, use the **show srp leafset** command in privileged EXEC configuration mode.

show srp leafset

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command displays leafset information for the current Proximity Engine (the local node). The current Proximity Engine must be part of a properly configured DHT network for leafset information about network members to be displayed.

Examples

The following example shows the output from **show srp leafset** when the current Proximity Engine is a standalone node and not a member of a DHT network:

```
ServiceRouter# show srp leafset

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
       I - Intransitive, W - wrapped

Leafset count: total 5, left 2, right 2

T    d2fc632c53c9ff1de8683e265386b09502791aedd65f28025fe7f64ad8cab2d9
    via sn-sj87 [ 172.20.168.87 ] :9000

ServiceRouter#
```

Table 2-71 describes the codes that **show srp leafset** uses in its output.

Table 2-71 Designations for Leafset Nodes

Code	Leafset Node Designation
T—local node	Proximity Engine where **show srp leafset** is issued.
L—leafset	Member of the leafset.
P—primary	Primary routing entry.
S—secondary	Secondary routing entry.
B—backup	Backup routing entry.
I—Intransitive	Intransitive routing entry.
W—wrapped	Wrapped routing entry.

The following example shows the output from **show srp leafset** command when the current Proximity Engine is a member of a DHT network consisting of seven nodes: the local node in the middle, three nodes on the left, and three nodes on the right.

```
ServiceRouter# show srp leafset

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
       I - Intransitive, W - wrapped
Leafset count: total 7, left 3, right 3
WPL  0e33b4fc00ea5e32b7323c2a712cc226fe4990430df6ac9a05d2a87ab67c9fae
    via sn-sj43 [ 172.20.168.43, 192.168.20.10, 192.168.86.10 ] :9000,
1.772254 ms, 00:00:08
PL   b5ca21563f5b938e46e2cb8f33a148ae00a1f6666f2a5eb735b7ed90c012c882
    via sn-sj82 [ 172.20.168.82, 192.168.82.82, 192.168.86.82 ] :9000,
0.392633 ms, 00:00:08
PL   c89908f53cc3ab6bc6065fd545341e9868cab7dcf852eaa346dd470011fcff1d
    via sn-sj89 [ 172.20.168.89 ] :9000, 0.352768 ms, 00:00:08
T    e966a1daec3ef3f1a81fec0e46338ae66eb7d154341e3a20fef0c5d2e8a0aabf
    via sn-sj87 [ 172.20.168.87 ] :9000
PL   0e33b4fc00ea5e32b7323c2a712cc226fe4990430df6ac9a05d2a87ab67c9fae
    via sn-sj43 [ 172.20.168.43, 192.168.20.10, 192.168.86.10 ] :9000,
1.772254 ms, 00:00:08
WPL  b5ca21563f5b938e46e2cb8f33a148ae00a1f6666f2a5eb735b7ed90c012c882
    via sn-sj82 [ 172.20.168.82, 192.168.82.82, 192.168.86.82 ] :9000,
0.392633 ms, 00:00:08
WPL  c89908f53cc3ab6bc6065fd545341e9868cab7dcf852eaa346dd470011fcff1d
    via sn-sj89 [ 172.20.168.89 ] :9000, 0.352768 ms, 00:00:08

ServiceRouter#
```

Related Commands

Command	Description
bootstrap-node	Configures a bootstrap node IP address.
domain	Sets the domain ID for the SRP.

show srp memory

To display SRP memory usage information, use the **show srp memory** command in privileged EXEC configuration mode.

show srp memory

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command displays SRP memory usage information.

Examples

The following example shows the output from **show srp memory** command:

```
ServiceRouter# show srp memory

SRP memory usage:
Type             Size      Count        HWM       Slab   Overhead      Total
Packet          65536          2          0          0          0     131072
Operation         192         92          0          0          0      18566
Sync              120          0          0          0          0          0
Pending           104          0          0          0          0          0
Mcast Pend         40          0          0          0          0          0
Proximity         104          0          0          0          0          0
To IPPC           208          0          0          0          0          0
Neighbor          384          2          2        128      48560      49328
Neighbor EP       134          0          0          0        128        128
Timer CTX          16         16         16         64        944       1200
Packet Addr        32          0          2          0        128        128
Subscriber        240          2          2         64      15056      15536
Seq Req            88          0          0          0        128        128
WorkQ              32          0          0          0        128        128
Total:                                                     65072     216214

ServiceRouter#
```

Related Commands

Command	Description
show srp process	Displays the basic configurations for SRP.

show srp multicast database

To display multicast database information for an SRP process, use the **show srp multicast database** command in privileged EXEC configuration mode.

show srp multicast database [*group_id* | **brief** | **statistics**]

Syntax Description

group_id	DHT key in hexadecimal format that identifies a group descriptor to be fetched from the multicast database.
brief	Displays brief information for each group descriptor in the database, including the DHT key, Type, Entity Type, Size, and the initial part of the Element Data in Element 0 of the descriptor.
statistics	Displays the number of entries (including deleted entries) in the multicast database.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command is used to display information saved in the multicast database. Without specifying any key or argument, **show srp multicast database** displays a summary of the multicast database. The summary contains the DHT key and size for each descriptor and the total number of active group descriptors in the database. By providing the DHT key in hexadecimal format or various filtering arguments, you can filter through the multicast database or a particular group descriptor to obtain desired information.

Examples

The following example is sample output from the **show srp multicast database** command when it is issued with no keywords or arguments:

```
ServiceRouter# show srp multicast database

DHT KEY                                                                 : SIZE
12300000000000000000000000000000000000000000000000000000000000000000: 1003
44440000000000000000000000000000000000000000000000000000000000000000: 522
77700000000000000000000000000000000000000000000000000000000000000000: 523
99900000000000000000000000000000000000000000000000000000000000000000: 307
c1898f9a8b69c3912f0fe8fecac30818fab24385fa8a1d37a8ffd193cf3eeebc: 124
Total                        5 active item(s) in the database

ServiceRouter#
```

The preceding example shows that there are five active entries in the database. If a descriptor is active (has not been deleted), its size is displayed. If a descriptor has been deleted, DELETED is displayed in the SIZE field of the descriptor. If the descriptor database is empty, the following output is displayed:

```
ServiceRouter# show srp multicast database
```

```
DHT KEY                                                                 : SIZE
Total                        0 active item(s) in the database

ServiceRouter#
```

The following is sample output from the **show srp multicast database** command when it is issued with the optional argument *group_id.* In this example, the DHT key for *group_id* is 4444:

```
ServiceRouter# show srp multicast database 4444

Getting database entry for
4444
Entity key:
4444000000000000000000000000000000000000000000000000000000000000
Entity rec type:          103     Entity total length: 522
Entity type:         22222222     Entity flags:        0
--------------- Element 0        (main)-----------------
Element ID: main
  Element total len          65   ID len:      0
  Delete Time: 0000000000000000
  Flags  0
  Last Update: Tue Feb 12 21:47:20 2008 (47b213e8ec98be67)
  Expiration : Thu Mar 13 21:47:20 2008 (47d9a0e8ec980000)
  Element data len:          25
  Element data:
    Content Acquirerquence number: 0
    Data: test
--------------- Element 1        (mcast)-----------------
Element ID: "....U.......(# .."(95160500550106090000000028230000)
  Element total len         123   ID len:      16
  Last Update: Tue Feb 12 21:48:14 2008 (47b2141e24526623)
  Expiration : Thu Mar 13 21:48:14 2008 (47d9a11e24520000)
  Element data len:          67
  Element data:
    Content Acquirerquence number: 1
    Sender ID: d2fc632c53c9ff1de8683e265386b09502791aedd65f28025fe7f64ad8cab2d9
    Data: hello1
--------------- Element 2        (mcast)-----------------
Element ID: "....r@......(# .."(9916050072401b1f0000000028230000)
  Element total len         123   ID len:      16
  Last Update: Tue Feb 12 21:48:18 2008 (47b214227ce17ea3)
  Expiration : Thu Mar 13 21:48:18 2008 (47d9a1227ce10000)
  Element data len:          67
  Element data:
    Content Acquirerquence number: 2
    Sender ID: d2fc632c53c9ff1de8683e265386b09502791aedd65f28025fe7f64ad8cab2d9
    Data: hello2
--------------- Element 3        (mcast)-----------------
Element ID: ".............(# .."(b0160500ae9e151c0000000028230000)
  Element total len         123   ID len:      16
  Last Update: Tue Feb 12 21:48:41 2008 (47b21439709c703b)
  Expiration : Thu Mar 13 21:48:41 2008 (47d9a139709c0000)
  Element data len:          67
  Element data:
    Content Acquirerquence number: 3
    Sender ID: d2fc632c53c9ff1de8683e265386b09502791aedd65f28025fe7f64ad8cab2d9
Data: hello3

ServiceRouter#
```

In the preceding example, the output is detailed information saved for the multicast group 4444 including the following:

- Multicast group 4444 has a record type 103.
- Its Entity Type is 22222222, which means this is a group-type descriptor.
- Its total length is 522 bytes.
- It has zero Entity Flags. Entity flags are not currently used.
- It has four elements:
  - Element 0 is the main element whose Element Data field saves group topic information instead of messages received by this group.
  - Other elements are created for saving messages received by the group.

Related Commands

Command	Description
clear srp group messages	Deletes all locally stored messages sent to a multicast group in the service routing layer.

show srp neighbor

To display SRP neighbor information, use the **show srp neighbor** command in privileged EXEC configuration mode.

show srp neighbor [**detail** | **down**]

Syntax Description

detail	Displays detailed information for each neighbor.
down	Displays the information of down neighbor entries.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command displays SRP neighbor information. The current Proximity Engine must be part of a properly configured DHT network for neighbor information about current network members to be displayed.

If the keyword **down** is specified, **show srp neighbor** displays down neighbors. These are Proximity Engines that are members of a DHT network the local Proximity Engine previously belonged to.

Examples

In the following example, assume a standalone Proximity Engine sn-sj87, and a two-node network consisting of Proximity Engine sn-sj81 and Proximity Engine sn-sj85. The **show srp neighbor** command is run from sn-sj87 before it is connected to the two-node network:

```
ServiceRouter# show srp neighbor

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
       I - Intransitive, D - delay, H - hold time

Number of neighbors in the database: 0
```

In the preceding example, sn-sj87 does not have any neighbor in the database.

In the following example, after sn-sj87 is added to the network, **show srp neighbor** is issued again. From the following output, we can see that sn-sj87 has two neighbors, sn-sj81 and sn-sj85:

```
ServiceRouter# show srp neighbor

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
       I - Intransitive, D - delay, H - hold time

Number of neighbors in the database: 2

PL  8886822171add71887d54107c266d814b605eaa0d5cc9b54b9160a137f4355d1
    via sn-sj81 [ 172.20.168.81 ] :9000, D=0.339605 ms,
    H=00:00:07
PL  9f752f56f347ca8fcc40a4e09b645f9b4c9b71c73401083f4c04920b30215b0a
via sn-sj85 [ 172.20.168.85, 192.168.20.85, 192.168.86.85 ] :9000,
D=0.379999 ms, H=00:00:09
```

To see details of these two neighbors, issue the **show srp neighbor detail** command:

```
ServiceRouter# show srp neighbor detail

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
       I - Intransitive
       D - delay, H - hold time, U - up time
       S_SEQ - send seq no., R_SEQ - receive seq. no.
       S_SID - send session id, R_SID - receive session id,
       R_Q - Receive Queue, T_Q - Transmit Queue.
Number of neighbors in the database: 2
PL  8886822171add71887d54107c266d814b605eaa0d5cc9b54b9160a137f4355d1
    via sn-sj81 [ 172.20.168.81 ] :9000, D=0.302328 ms,
    H=00:00:08, U=02:15:53, S_SEQ=1, R_SEQ=0, S_SID=148214958, R_SID=0
PL  9f752f56f347ca8fcc40a4e09b645f9b4c9b71c73401083f4c04920b30215b0a
via sn-sj85 [ 172.20.168.85, 192.168.20.85, 192.168.86.85 ] :9000,
D=0.379999 ms, H=00:00:10, U=01:45:42, S_SEQ=0, R_SEQ=0,
S_SID=2134859630, R_SID=0
```

The following example illustrates the usage of **show srp neighbor down**. Assume that a four-node network consists of Proximity Engines sn-sj43, sn-sj88, sn-sj44, and sn-sj87. From sn-sj87, the **show srp neighbor down** command can be used to confirm this, as shown by the following output:

```
ServiceRouter# show srp neighbor

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
       I - Intransitive, D - delay, H - hold time
Number of neighbors in the database: 3
PLI 0e33b4fc00ea5e32b7323c2a712cc226fe4990430df6ac9a05d2a87ab67c9fae
    via sn-sj43 [ 192.168.86.43 ] :9000, D=0.439602 ms,
   H=00:00:03
PL  2a2db308fd3dc172940a7902a4db7c16c98c3a32e1b048005bce1e832b6d056f
    via sn-sj88 [ 192.168.86.88 ] :9000, D=0.405537 ms,
   H=0.553618
PL  9a28755bba0228c7ac3d1be20d21a7a57c532eed9d5ffc5e1da2a9841e2e77a8
    via sn-sj44 [ 192.168.86.44 ] :9000, D=0.398474 ms,
   H=00:00:01

ServiceRouter# show srp neighbor down

Number of down neighbors in the database: 0
Next down neighbor write offset: 0
```

For the next example, assume that the domain ID for the local node (sn-sj87) is reconfigured so that it is detached from the network. The following output from **show srp neighbor down** now shows that all three neighbors are down:

```
ServiceRouter# show srp neighbor down
Number of down neighbors in the database: 3
Next down neighbor write offset: 3

9a28755bba0228c7ac3d1be20d21a7a57c532eed9d5ffc5e1da2a9841e2e77a8
   via sn-sj44 [ 192.168.86.44 ] :9000, 0.000 ms, no-timer
0e33b4fc00ea5e32b7323c2a712cc226fe4990430df6ac9a05d2a87ab67c9fae
   via sn-sj43 [ 192.168.86.43 ] :9000, 0.000 ms, no-timer
2a2db308fd3dc172940a7902a4db7c16c98c3a32e1b048005bce1e832b6d056f
   via sn-sj88 [ 192.168.86.88 ] :9000, 0.000 ms, no-timer
```

Related Commands

Command	Description
bootstrap-node	Configures a bootstrap node IP address.
domain	Sets the domain ID for an SRP.

show srp process

To display the basic configurations for SRP, use the **show srp process** command in privileged EXEC configuration mode.

show srp process

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command displays SRP process information.

Examples

The following example shows sample output from **show srp process** when it is run from Proximity Engine sn-sj87.

```
ServiceRouter# show srp process

Process:
  Domain: 0
  Node Id: d2fc632c53c9ff1de8683e265386b09502791aedd65f28025fe7f64ad8cab2d9
  Host name: sn-sj87
  Port: 9000
  Interfaces running SRP:
     *GigabitEthernet 1/0
  Bootstrap host name: 172.20.168.85, address: 172.20.168.85, port: 9000
  Database Mirroring: Disabled
  # of storages requested for mirroring: 2
  # of storages used for mirroring     : 1

ServiceRouter#
```

Related Commands

Command	Description
show srp memory	Displays SRP memory usage information.

show srp replica-set

To display the replica set information for a Proximity Engine, use the **show srp replica-set** command in privileged EXEC configuration mode.

show srp replica-set

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command displays SRP replica set information.

To use this command to show a replica set, a network needs to be formed by properly configuring a bootstrap node and domain ID.

Examples

The following examples show sample output from **show srp replica-set**. For the first example, assume a standalone Proximity Engine sn-sj87 and a two-node network consisting of Proximity Engine sn-sj81 and Proximity Engine sn-sj85. The **show srp replica-set** command is issued from sn-sj87 before it is connected to the two-node network:

```
ServiceRouter# show srp replica-set

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
       I - intransitive, R - Replicate Set, A - active

key(part)         address              type  state
-------------------------------------------------

308fe23f...       EE7-CDE205-8:9000    PL    Active
5c71ac1e...       EE7-CDE205-10:9000   PL    Active
feb5784c...->     SN-CDSM:9000         local None
ServiceRouter#
```

Related Commands

Command	Description
show srp leafset	Displays SRP leafset information,
show srp neighbor	Displays SRP neighbor information

show srp route

To display route information for a Proximity Engine to its neighbor nodes on the same DHT network, use the **show srp route** command in privileged EXEC configuration mode.

show srp route [**backup | statistics**]

Syntax Description

backup	Displays entries, including backup entries.
statistics	Displays statistics information.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command displays route information for a Proximity Engine to its neighbor nodes on the same DHT network.

To use this command to show route entries, a network needs to be formed by properly configuring a bootstrap node and domain ID.

Examples

The following examples show sample output from **show srp route**. For the first example, assume a standalone Proximity Engine sn-sj87 and a two-node network consisting of Proximity Engine sn-sj81 and Proximity Engine sn-sj85. The **show srp route** command is issued from sn-sj87 before it is connected to the two-node network. The output shows no srp route information, as is expected for a standalone Proximity Engine:

```
ServiceRouter# show srp route

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
       I - Intransitive
```

For the following example, assume that Proximity Engine sn-sj87 has joined the two-node network consisting of Proximity Engine sn-sj81 and Proximity Engine sn-sj85. The output shows that sn-sj87 has route information to its two neighbors, sn-sj81 and sn-sj85.

```
ServiceRouter# show srp route

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
       I - Intransitive
PL  8/4 via 8886822171add71887d54107c266d814b605eaa0d5cc9b54b9160a137f4355d1
    sn-sj81 [ 172.20.168.81 ] :9000, 0.301080 ms, 00:00:09
PL  9/4 via 9f752f56f347ca8fcc40a4e09b645f9b4c9b71c73401083f4c04920b30215b0a
sn-sj85 [ 172.20.168.85, 192.168.20.85, 192.168.86.85 ] :9000, 0.382097 ms,
00:00:08
```

The **show srp route** command shows only primary routing table entries. In the SRP routing table, there are backup routes as well. To display the backup routes as well as the primary routes, use the command **show srp route backup** command:

```
ServiceRouter# show srp route backup

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
       I - Intransitive
PL  8/4 via 8886822171add71887d54107c266d814b605eaa0d5cc9b54b9160a137f4355d1
    sn-sj81 [ 172.20.168.81 ] :9000, 0.301080 ms, 00:00:07
PL  9/4 via 9f752f56f347ca8fcc40a4e09b645f9b4c9b71c73401083f4c04920b30215b0a
sn-sj85 [ 172.20.168.85, 192.168.20.85, 192.168.86.85 ] :9000, 0.382097 ms,
00:00:10

ServiceRouter#
```

Because there is no backup route in this small three-node network, **show srp route backup** displays the same results as **show srp route**. This can be confirmed by issuing the **show srp route statistics** command as shown in the following example. From the following output, we can confirm that are total two routes in the routing table, one appearing in cell 8 row 0 (which is the route via sn-sj81) and the other appearing in cell 9 row 0 (which is the route via sn-sj85).

```
ServiceRouter# show srp route statistics

Total routes: 2
Entries that share my prefix: 0
Last nonempty row: 0

ServiceRouter#
```

Related Commands

Command	Description
show srp leafset	Displays SRP leafset information.
show srp neighbor	Displays SRP neighbor information.
show statistics srp	Displays SRP statistics information.

show srp subscribers

To display SRP multicast group subscriber information, use the **show srp subscribers** command in privileged EXEC configuration mode.

show srp subscribers

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command is used to check what multicast groups the Proximity Engine is currently subscribed to. If the Proximity Engine is not subscribed to any groups, there is no output.

Examples

In the following example, assume a standalone Proximity Engine sn-sj87:

1. The **show srp subscribers** command displays output showing that sn-sj87 is subscribed to one group (c1898f9a8b69c3912f0fe8fecac30818fab24385fa8a1d37a8ffd193cf3eeebc).
2. The local Proximity Engine (sn-sj87) subscribes to another existing multicast group (999).
3. The **show srp subscribers** displays output showing that sn-sj87 is subscribed two groups (c1898f9a8b69c3912f0fe8fecac30818fa b24385fa8a1d37a8ffd193cf3eeebc and 999).

```
ServiceRouter# show srp subscribers

c1898f9a8b69c3912f0fe8fecac30818fab24385fa8a1d37a8ffd193cf3eeebc
  Root node: d2fc632c53c9ff1de8683e265386b09502791aedd65f28025fe7f64ad8cab2d9
  Subscriber: 0x6891a0

ServiceRouter# show srp subscribers

999000000000000000000000000000000000000000000000000000000000000000000000
  Root node: 8886822171add71887d54107c266d814b605eaa0d5cc9b54b9160a137f4355d1
  Subscriber: 0x6891a0
c1898f9a8b69c3912f0fe8fecac30818fab24385fa8a1d37a8ffd193cf3eeebc
  Root node: d2fc632c53c9ff1de8683e265386b09502791aedd65f28025fe7f64ad8cab2d9

ServiceRouter#
```

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.

Command 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.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-72 describes the fields shown in the **show standby** display.

Table 2-72 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 keywords or arguments.

Command 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
! CDS 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
!
!
!
cdsm ip 4.0.8.10
cms enable
!
!
!
service-router service-monitor threshold wmt 50
service-router service-monitor number-of-samples wmt 5
service-router service-monitor sample-period wmt 15
qos device-policy-service enable
!
!
cache content max-cached-entries 1000
! End of CDS 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 aaa

To display SE access control list statistics, use the **show statistics access-lists 300** command in EXEC configuration mode.

show statistics aaa

Syntax Description

This command has no keywords or arguments.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-73 describes the fields shown in the **show statistics aaa** display.

Table 2-73 show statistics aaa Field Descriptions

Field	Description
Authentication and Authorization Statistics	
Number of access requests	The number of authentication and authorization requests issued from this server.
Number of access deny responses	The number of authentication and authorization deny responses received from remote AAA server.
Number of access allow responses	The number of authentication and authorization allow responses received from remote AAA server.
Accounting Statistics	
Number of access requests	The number of accounting requests issued from this server.
Number of access deny responses	The number of accounting deny responses received from remote AAA server.
Number of access allow responses	The number of accounting allow responses received from remote AAA server.

Related Commands

Command	Description
aaa	Specifies accounting, authentication and authorization methods.
show aaa	Displays the accounting, authentication and authorization configuration.

show statistics access-lists 300

To display SE access control list statistics, use the **show statistics access-lists 300** command in EXEC configuration mode.

show statistics access-lists 300

Syntax Description

This command has no keywords or arguments.

Command 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 2-74 describes the fields shown in the **show statistics access-lists 300** display.

Table 2-74 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 acquirer

To display SE acquirer channel statistics, use the **show statistics acquirer** command in EXEC configuration mode.

show statistics acquirer [**contents** {**delivery-service-id** *delivery_service_id* | **delivery-service-name** *delivery_service_name*} | **delivery-service-id** *delivery_service_id* | **delivery-service-name** *delivery_service_name* | **errors** {**delivery-service-id** *delivery_service_id* | **delivery-service-name** *delivery_service_name*} | **job-list** {**delivery-service-id** *delivery_service_id* | **delivery-service-name** *delivery_service_name*}]

Syntax Description

contents	(Optional) Displays the acquired contents of the specified channel.
delivery-service-id	Displays acquirer statistics for the specified delivery service ID.
delivery_service_id	Delivery service ID.
delivery-service-name	Displays acquirer statistics for the specified delivery service name.
delivery_service_name	Delivery service name.
errors	(Optional) Displays the acquisition error logs for the specified channel.
job-list	(Optional) Displays the job list statistics for the specified channel.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **show statistics acquirer** command displays acquirer statistics for all channels for which the SE is the Content Acquirer. The output of the command displays any manifest file parsing or fetch errors if any errors occur. It displays the total number of acquired objects, number of failed objects, and total disk space used by the acquired objects. When a channel ID or name is specified, acquirer statistics are displayed for that channel specified by ID or name.

The **show statistics acquirer contents** command displays all the acquired content, its size, and its last-modified time, specified by channel ID or name.

The **show statistics acquirer errors** command displays acquisition errors, if any, for the channel specified by ID or name. Manifest file parsing and fetch errors, as well as single item or crawler job errors, are displayed.

The **show statistics acquirer job-list** command displays the details of all the single items and crawler jobs for the channel specified by ID or name.

Table 2-75 describes the fields shown in the **show statistics acquirer** display.

Table 2-75 show statistics acquirer Field Descriptions

Field	Description
Statistics For Channel ID: ***channel-id***	
Delivery-service-id	Delivery service identification number.

Table 2-75 show statistics acquirer Field Descriptions (continued)

Field	Description
Delivery-service-name	Name of the delivery service.
Manifest	
Fetch Errors	Number of manifest file fetch errors.
Parsing Errors	Number of manifest file parsing errors.
Acquisition	
Total Number of Acquired Objects	Total number of acquired objects.
Total Size of Acquired Objects (Bytes)	Total size of acquired objects (in bytes).
Total Number of Failed Objects	Total number of failed objects.

Table 2-76 describes the fields shown in the **show statistics acquirer contents delivery-service-name** display.

Table 2-76 show statistics acquirer contents delivery-service-name Field Descriptions

Field	Description
Acquired Contents	
Modification Time	Local time the acquirer contents were modified.
Size	Size of the file.
URL	URL of the file.

Examples

The following example shows how to display the acquirer statistics for the Delivery Service name settur-ds:

```
ServiceEngine# show statistics acquirer contents deliver-service-name settur-ds
Querying Database.......

Contents Acquired for the Delivery Service Name :settur-ds
----------------------------------------

Acquired Contents:
----------------------

Modification Time : Fri Aug  1 06:08:26 2008
Size              : 128899758 Bytes
Url               : http://172.XX.XX.XX/300kbs.wmv


Modification Time : Wed May 21 08:58:17 2008
Size              : 174569021 Bytes
Url               : http://172.XX.XX.XX/1mbps.mov


Modification Time : Wed May 11 09:19:17 2011
```

```
Size              : 425468369 Bytes
Url               : http://172.XX.XX.XX/flash_1mbps.mp4


Modification Time : Mon Jun 20 10:15:37 2011
Size              : 22952732 Bytes
Url               : http://172.XX.XX.XX/sample.mpeg
```

Related Commands

Command	Description
acquirer (EXEC)	Starts or stops content acquisition on a specified acquirer delivery service.
clear statistics	Clears all statistical counters from the parameters given.
show acquirer	Displays the acquirer information and progress of content acquisition for a specified channel number or name.

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 keywords or arguments.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-77 describes the fields shown in the **show statistics admission** display.

Table 2-77 show statistics admission

Field	Description
QOS Admission Check	
Bypassed	Number of times admission control was turned off.
Attempts	Total number of admission attempts.
Succeeded	Total number of attempts that succeeded.
Failed	Total number of attempts that failed.
Best effort	
Attempts	Total number of attempts for Best Effort traffic.
Based on congestion	Attempts failed because disk is too busy.
Succeeded	Total attempts that succeeded.
Failed	
Too many sessions	Attempts failed because number of sessions is too high.
Average too low	Attempts failed because average bit rate is too low.
Soft guaranteed	
Attempts	Total attempts for SG traffic.
Succeeded	Total attempts that succeeded.
Failed	
Disk congestion	Total attempts that failed because of disk congestion.

Table 2-77 show statistics admission (continued)

Field	Description
BE would be too low	Total attempts that failed because BE traffic rate would become too low.
Over threshold	Total attempts that failed because SG total was over congestion threshold.
Hard guaranteed	
Attempts	Total attempts for HG traffic.
Succeeded	Total attempts that succeeded.
Failed	Total attempts that failed.
Hole management	
Bypassed	Total requests where hole management was turned off.
Succeeded	Total attempts that succeeded.
Failed	
fill too close	Total attempts that failed because an ongoing fill was too close to the request offset.
Hit data	
with active fill	Total attempts that hit data range with an active fill.
request range inside inactive fill	Total attempts that hit data and fully covered.
request range overlaps inactive fill	Total attempts that hit data and not fully covered.
Hit hole	
not aligned, 2 fills	Total attempts that hit hole, not play block aligned.
aligned, 1 fill	Hit hole but play block aligned.
too many fills	Hit hole but too many fills ongoing.
too many holes	
fill from start	Too many holes in file, bridging will occur from start of file.
active fill	Too many holes but an active fill will bridge hole.
fill from left	Too many holes, start fill to bridge hole from left.
Disk overload	
Misc errors	
Incorrect QoS type	The QoS type may not be set to one of the following: • Best Effort • Soft Guaranteed • Hard Guaranteed
Hole management	A kernel error because of one of the following: • block_bytes = 0 • get_fill_map() failed.

show statistics authsvr

To view the Authentication Server statistics, use the **show statistics authsvr** command in EXEC configuration mode.

show statistics authsvr {**delivery-service-id** *num* {**detail** | **geo** | **ip** | **rules**} | **global**}

Syntax Description

delivery-service-id	Delivery service ID.
num	Displays delivery service statistics (0 to 4294967295).
detail	Displays detail statistics for all authorization types.
geo	Displays geographical authorization statistics.
ip	Displays IP authorization statistics.
rules	Displays rules authorization statistics.
global	Displays Authentication Server global statistics.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The output of the **show statistics authsvr** command displays Rules statistics based on the rules configured through the XML. If Rule_Allow is configured, then the statistics for Rule_Allow must be incremented whether or not any other rule is configured. If the Rule_Allow or Rule_Block is not configured but Rule_UrlRewrite is configured, then the statistics of Rule_UrlRewrite are incremented. Similarly, if the Rule_Block is configured along with Rule_UrlRewrite, then the statistics of Rule_Block and Rule_UrlRewrite are incremented.

When Unknown Server Requests is enabled, a request for an unknown server increments both the Allowed counter and the Unknown Server Allowed counter. When Unknown Server Request is disabled, a request for an unknown server increments both the Blocked counter and the Unknown Server Blocked counter.

The **show statistics authsvr delivery-service-id** command displays statistics for each delivery service and for each rule in the delivery service. All the statistics are based on the Authsvr Rules configured in the XML file for a particular delivery service.

Table 2-78 describes the fields shown in the **show statistics authsvr delivery-service-id detail** display.

Table 2-78 show statistics authsvr delivery-service-id detail Command Field Descriptions

Field	Description
IP Statistics	IP authorization statistics.
Allow	This field increments when Unknown Server Request is enabled.
Block	This field increments when Unknown Server Request is disabled.
Geo Statistics	Geographical authorization statistics.
Allow	This field increments when Unknown Server Request is enabled.
Block	This field increments when Unknown Server Request is disabled.
Rules Statistics	Rules authorization statistics.
Rule Allow	Number of authorization requests applied on Rule Allow.
Rule Block	Number of Rule Block statistics.
Rule Forced Revalidate	Number of Rule Forced Revalidate statistics.
Rule No Cache	Number of Rule No Cache statistics.
Rule SWF File Validate	Number of Rule (FMS) SWF File Validate statistics.
Rule URL Redirect	Number of Rule URL Redirect statistics.
Rule URL Resolve	Number of Rule URL Resolve statistics.
Rule URL Rewrite	Number of Rule URL Rewrite statistics.

Table 2-79 describes the fields shown in the **show statistics authsvr global** display.

Table 2-79 show statistics authsvr global Command Field Descriptions

Field	Description
Allowed	This field increments when Unknown Server Request is enabled.
Blocked	This field increments when Unknown Server Request is disabled.
Unknown Server Allowed	This field increments when Unknown Server Request is enabled.
Unknown Server Blocked	This field increments when Unknown Server Request is disabled.
Errors	This field increments when errors occur.

Examples

The following shows how to display the Authentication Server delivery service ID detail statistics:

```
ServiceEngine# show statistics authsvr delivery-service-id 1 detail

IP Statistics
----------------
    Allow               :  200
    Block               :  10
```

```
Geo Statistics
-------------------
    Allow               :  23
    Block               :  10

Rules Statistics
----------------------
    Rule_Allow          :  134
    Rule_Block          :  23
    Rule_ForcedReValidate:  12
    Rule_NoCache        :  16
    Rule_SwfFileValidate :  5
    Rule_UrlRedirect    :  7
    Rule_UrlResolve     : 10
    Rule_UrlRewrite     :  3
ServiceEngine#
```

The following shows how to display the Authentication Server global statistics:

```
ServiceEngine# show statistics authsvr global

Authserver Statistics
---------------------
Allowed                :                  4329108
Blocked                :                        0
Unknown Server Allowed :                       10
Unknown Server Blocked :                        0
Errors                 :                        0
ServiceEngine#
```

Related Commands

Command	Description
authsvr	Enables and configures the Authorization server.
show authsvr	Displays the status of the Authorization server.

show statistics cdn-select

To view the CDN Selector statistics, use the **show statistics cdn-select** command in EXEC configuration mode.

show statistics cdn-select summary

Syntax Description

summary	Displays summary statistics for the CDN Selector.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following is sample CDN Selector statistics:

```
ServiceRouter# show statistics cdn-select summary

----- CDN Selector Summary Statistics -----

Requests Received                 :                 0
Requests Redirected (3rd party)   :                 0
Requests Routed (CDS-IS)          :                 0
Requests Not Redirected           :                 0
  CDN Errors                      :                 0

ServiceRouter#
```

Related Commands

Command	Description
cdn-select	Enables the CDN Selector for third-party service selection.
geo-location-server	Redirects requests to different Content Delivery Networks based on the geographic location of the client.
show cdn-select	Displays the status of the CDN Selector.

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.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-80 describes the **show statistics cdnfs** command fields displayed in the command output.

Table 2-80 show statistics cdnfs Fields

Field	Description
Size of physical file system	Physical disk size of the 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.
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.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 2-81 describes the **show statistics content-mgr** command fields displayed in the command output.

Table 2-81 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.
Slow Scan Cache Child Count	Count of cached child content (WMT/MS) 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.

Table 2-81 show statistics content-mgr Fields (continued)

Field	Description
Eviction Protect Skip Count	Number of contents skipped since it is protected by eviction protection.
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.