



Module Commands for Cisco Unified SIP Proxy

Last Updated: November 1, 2020

- [backup \(module\)](#)
- [backup category](#)
- [backup security key](#)
- [backup security enforced](#)
- [backup security protected](#)
- [backup server authenticate](#)
- [clock timezone](#)
- [continue](#)
- [copy core](#)
- [copy ftp:](#)
- [copy ftp: configuration active](#)
- [hostname](#)
- [interface gigabitethernet](#)
- [ip address](#)
- [ip broadcast-address](#)
- [ip tcp keepalive-time](#)
- [log console](#)
- [log console monitor](#)
- [log server](#)
- [log trace boot](#)
- [log trace buffer save](#)
- [ntp server](#)
- [offline](#)
- [reload](#)
- [restore](#)
- [restore factory default](#)

- `security ssh known-hosts`
- `show backup`
- `show backup history`
- `show backup server`
- `show clock detail`
- `show interfaces`
- `show logs`
- `show ntp associations`
- `show ntp servers`
- `show ntp source`
- `show ntp status`
- `show process`
- `show running-config`
- `show security ssh known-hosts`
- `show software`
- `show trace log`
- `show startup-config`
- `show version`
- `snmp-server community`
- `snmp-server contact`
- `snmp-server enable traps`
- `snmp-server host`
- `snmp-server location`
- `write`

backup (module)

To set the backup parameters, use the **backup** command in module configuration mode. To delete the number of revisions or the backup server URL, use the **no** form of this command.

backup { **revisions** *number* | **server url** *ftp-url* **username** *ftp-username* **password** *ftp-password* }

no backup { **revisions** *number* | **server url** *ftp-url* }

Syntax Description

revisions <i>number</i>	Number of revision files stored in the Cisco Unified SIP Proxy database.
server url <i>ftp-url</i>	URL to the FTP server where the backup files are to be stored.
username <i>ftp-username</i>	User ID needed to access the FTP server.
password <i>ftp-password</i>	Password needed to access the FTP server.

Command Default

None

Command Modes

Module configuration (config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Set these parameters before backing up any files.

Consider the amount of storage space that each backup file requires when setting the number of files to store. When the number is reached, the next backup file overwrites the oldest stored backup file.

The system automatically numbers and dates the backup files and identifies the revision number in a **backupid** field. Reference this backup ID value when restoring a file.

Performing different backup types at various times causes different backup IDs for data backups and configuration backups. For example, the last data backup ID might be 3 and the last configuration backup might be 4. Performing an **all** backup might result in a backup ID of 5 for both data and configuration. See the [backup category](#) command for information about different backup types.



Note

CUSP currently does not support secure FTP (SFTP) backup or restore.

There are two **backup** commands: this command in module configuration mode, and another command in offline EXEC mode.

If the **backup** (module) command is unset, and the **backup** (offline EXEC) command is unset, the command fails.

If the **backup** (module) command is set, and the **backup** (offline EXEC) command is unset, the **backup** (module) command is used

backup (module)

If the **backup (module)** command is unset, and the **backup (offline EXEC)** command is set, the **backup (offline EXEC)** command is used.

If both commands are set, the **backup (offline EXEC)** command is used.

Examples

The following example sets 7 revisions on FTP server /branch/vmbackups.

```
se-10-0-0-0> enable
se-10-0-0-0# configure terminal
se-10-0-0-0(config)> backup revisions 7
se-10-0-0-0(config)> backup server url ftp://branch/vmbackups username admin password
mainserver
```

Related Commands

Command	Description
backup category	Specifies the type of data to be backed up.
show backup history	Displays statistics for backed-up files.
show backup server	Displays the FTP server designated to store backup files.

backup category

To specify the type of data to be backed up, use the **backup category** command in offline mode.

backup category {all | configuration | data}

Syntax Description	all	Backs up all data.
	configuration	Backs up only system and application settings.
	data	Backs up only voice-mail messages and application data.

Command Default All data is backed up.

Command Modes Offline

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use this command to indicate the type of Cisco Unified SIP Proxy data.

Examples The following examples illustrate all the backup categories:

```
se-10-0-0-0> enable
se-10-0-0-0# offline
!!!WARNING!!!: Putting the system offline will terminate all active calls.
Do you wish to continue[n]? : y
se-10-0-0-0(offline)# backup category all
se-10-0-0-0(offline)# continue
se-10-0-0-0#
```

```
se-10-0-0-0> enable
se-10-0-0-0# offline
!!!WARNING!!!: Putting the system offline will terminate all active calls.
Do you wish to continue[n]? : y
se-10-0-0-0(offline)# backup category configuration
se-10-0-0-0(offline)# continue
se-10-0-0-0#
```

```
se-10-0-0-0> enable
se-10-0-0-0# offline
!!!WARNING!!!: Putting the system offline will terminate all active calls.
Do you wish to continue[n]? : y
se-10-0-0-0(offline)# backup category data
se-10-0-0-0(offline)# continue
se-10-0-0-0#
```

Related Commands	Command	Description
	continue	Activates the backup or restore process.
	offline	Initiates Cisco Unified SIP Proxy offline mode.
	show backup history	Displays details about backed-up files.
	show backup server	Displays details about the backup server.

backup security key

To create or delete the master key used for encrypting and signing the backup files, use the **backup security key** command in module configuration mode.

backup security key {generate | delete}

Syntax Description	generate	Creates a master key.
	delete	Deletes a master key.

Command Default No key is configured.

Command Modes Module configuration (config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use the **backup security key** command in Cisco Unified SIP Proxy configuration mode to create or delete the master key used for encrypting and signing the backup files. When creating a backup security key, you are prompted to enter the password from which the key will be derived.

This command is not saved in the startup configuration when you use the **write** command.

Examples The following example creates a master key:

```
se-10-0-0-0(config)> backup security key generate
Please enter the password from which the key will be derived: *****
```

The following example deletes a master key:

```
se-10-0-0-0(config)> backup security key delete
You have a key with magic string cfbdbbee
Do you want to delete it [y/n]?:
```

Related Commands	Command	Description
	backup security enforced	Specifies that only protected and untampered backup files can be restored.
	backup security protected	Enables secure mode for backups.
	write	Copies the running configuration to the startup configuration.

backup security enforced

To specify that only protected and untampered backup files can be restored, use the **backup security enforced** command in Cisco Unified SIP Proxy configuration mode.

backup security enforced

Syntax Description

This command has no arguments or keywords.

Command Default

All of the following types of backup files are restored:

- Unprotected (clear)
- Protected
- Untampered

Command Modes

Module configuration (config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Before you can use this command, you must generate a backup security key by using the **backup security key generate** command.

Use the **backup security enforced** command in Cisco Unified SIP Proxy configuration mode to specify that only protected and untampered backup files can be restored. By default, the system also restores unprotected (clear) backup files, as protected backup files and untampered backup files.

Examples

The following example specifies that only protected and untampered backup files can be restored:

```
se-10-0-0-0# configure terminal
se-10-0-0-0(config)# backup security enforced
```

Related Commands

Command	Description
backup security key generate	Creates or deletes the master key used for encrypting and signing the backup files.
backup security protected	Enables secure mode for backups.

backup security protected

To enable secure mode for backups, use the **backup security protected** command in Cisco Unified SIP Proxy configuration mode.

backup security protected

Syntax Description This command has no arguments or keywords.

Command Default Backup files are stored in unprotected mode on the remote server.

Command Modes Module configuration (config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Before using this command, you must generate backup security key by using the **backup security key generate** command.

Use the **backup security protected** command in Cisco Unified SIP Proxy configuration mode to enable secure mode for backups. In secure mode, all backup files are protected using encryption and a signature.

Examples The following example enables secure mode for backups:

```
se-10-0-0-0# configure terminal
se-10-0-0-0(config)# backup security protected
```

Related Commands	Command	Description
	backup security enforced	Specifies that only protected and untampered backup files can be restored.
	backup security key generate	Creates or deletes the master key used for encrypting and signing the backup files.

backup server authenticate

To retrieve the fingerprint of the backup server's host key, use the **backup server authenticate** command in module configuration mode.

backup server authenticate

Syntax Description This command has no arguments or keywords.

Command Default This command has no default value.

Command Modes Module configuration (config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use the **backup server authenticate** command in module configuration mode to retrieve the fingerprint of the backup server's host key. Before using this command, users must configure the backup server URL and the login credential. The backup server URL must start with "ftp://." After the fingerprint is retrieved from the backup server, the system prompts the user for confirmation.

If this command is accepted, the fingerprint is stored in the form of "backup server authenticate fingerprint *fingerprint-string*" in the running configuration. This command is not saved in the startup configuration when you use the **write** command.

Examples The following example retrieves the fingerprint of the backup server's host key:

```
se-10-0-0-0# configure terminal
se-10-0-0-0(config)# backup server authenticate
The fingerprint of host 10.30.30.100 (key type ssh-rsa) is:
    a5:3a:12:6d:e9:48:a3:34:be:8f:ee:50:30:e5:e6:c3
Do you want to accept it [y/n]?
```

Related Commands	Command	Description
	security ssh known-hosts	Configures the MD5 fingerprint of the SSH server's host key.
	show security ssh	Displays a list of configured SSH servers and their fingerprints.
	write	Copies the running configuration to the startup configuration.

clock timezone

To set the time zone for the Cisco Unified SIP Proxy service module, use the **clock timezone** command in module EXEC mode.

clock timezone [*time-zone*]

Syntax Description	<i>time-zone</i> (Optional) Specifies the time zone of the local branch.
---------------------------	--

Command Modes	Module EXEC (>)
----------------------	-----------------

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines	<p>The configured NTP server provides the date-stamp system and application functions. The clock timezone command specifies the local time zone where Cisco Unified SIP Proxy is installed.</p> <p>If you know the phrase for the time-zone, enter it for the <i>time-zone</i> value. If you do not know the time zone phrase, leave the <i>time-zone</i> value blank and a series of menus appear to guide you through the time zone selection process.</p>
-------------------------	---

Examples	To select United States Pacific Time using the time-zone menu:
-----------------	--

```
se-10-0-0-0(config)> clock timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa           4) Arctic Ocean       7) Australia        10) Pacific Ocean
2) Americas         5) Asia               8) Europe
3) Antarctica       6) Atlantic Ocean    9) Indian Ocean
>? 2
Please select a country.
1) Anguilla         18) Ecuador           35) Paraguay
2) Antigua & Barbuda 19) El Salvador       36) Peru
3) Argentina        20) French Guiana    37) Puerto Rico
4) Aruba            21) Greenland        38) St Kitts & Nevis
5) Bahamas          22) Grenada          39) St Lucia
6) Barbados         23) Guadeloupe       40) St Pierre & Miquelon
7) Belize           24) Guatemala        41) St Vincent
8) Bolivia          25) Guyana            42) Suriname
9) Brazil           26) Haiti             43) Trinidad & Tobago
10) Canada           27) Honduras         44) Turks & Caicos Is
11) Cayman Islands  28) Jamaica           45) United States
12) Chile            29) Martinique       46) Uruguay
13) Colombia        30) Mexico            47) Venezuela
14) Costa Rica      31) Montserrat       48) Virgin Islands (UK)
15) Cuba            32) Netherlands Antilles 49) Virgin Islands (US)
16) Dominica        33) Nicaragua
17) Dominican Republic 34) Panama
>? 45
Please select one of the following time zone regions.
```

clock timezone

```

1) Eastern Time
2) Eastern Time - Michigan - most locations
3) Eastern Time - Kentucky - Louisville area
4) Eastern Standard Time - Indiana - most locations
5) Central Time
6) Central Time - Michigan - Wisconsin border
7) Mountain Time
8) Mountain Time - south Idaho & east Oregon
9) Mountain Time - Navajo
10) Mountain Standard Time - Arizona
11) Pacific Time
12) Alaska Time
13) Alaska Time - Alaska panhandle
14) Alaska Time - Alaska panhandle neck
15) Alaska Time - west Alaska
16) Aleutian Islands
17) Hawaii
>? 11

```

The following information has been given:

```

United States
Pacific Time

```

```

Therefore TZ='America/Los_Angeles' will be used.
Local time is now:      Fri Dec 24 10:41:28 PST 2004.
Universal Time is now:  Fri Dec 24 18:41:28 UTC 2004.
Is the above information OK?
1) Yes
2) No
>? 1
se-10-0-0(config)>

```

To select United States Pacific Time using the timezone name:

```
se-10-0-0-0(config)> clock timezone Americas/Los_Angeles
```

Related Commands

Command	Description
ntp server	Specifies the NTP server.
show clock detail	Displays the clock details.

continue

To return the Cisco Unified SIP Proxy system to online mode, use the **continue** command in module offline mode.

continue

Syntax Description This command has no arguments or keywords.

Command Default The system remains in offline mode.

Command Modes Module offline (offline)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines This command returns the Cisco Unified SIP Proxy system to the previous online mode, such as after a backup procedure or to discontinue a restore to factory defaults. The system begins processing new calls and voice messages. Cisco Unified SIP Proxy still routes calls in offline mode.

Examples The following example illustrates the use of the **continue** command in the backup procedure:

```
se-10-0-0-0# offline
!!!WARNING!!!: Putting the system offline will terminate all active calls.
Do you wish to continue[n]? : y
se-10-0-0-0(offline)# backup category data
se-10-0-0-0(offline)# continue
se-10-0-0-0#
```

Related Commands	Command	Description
	backup	Identifies the data to be backed up.
	offline	Terminates all active calls and prevents new calls from connecting to the Cisco Unified SIP Proxy application.
	reload	Restarts the Cisco Unified SIP Proxy system.
	restore	Identifies the file to be restored.
	restore factory default	Restores the system to factory default values.

copy core

To copy a core file to a remote URL, use the **copy core** command in module EXEC mode.

copy core *core-name* **url** *ftp/http url*

Syntax Description	<i>core-name</i>	Core filename
	<i>ftp/http url</i>	FTP/HTTP address

Command Default	None
------------------------	------

Command Modes	Module EXEC (>)
----------------------	-----------------

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines	The standard FTP URL format is supported:
	<code>ftp://[user-id:ftp-password@]ftp-server-address[/directory]</code>

Examples	The following command copies the core to ftp://anonymous@ftp.nowhere.com/pub/.
	<code>se-Module(exec-helloworld)> copy core test-file2 url ftp://anonymous@ftp.example.com/pub/</code>

Related Commands	Command	Description
	copy ftp:	Copies a new configuration from an FTP server to another Cisco Unified SIP Proxy location.
	show cores	Displays all core files.

copy ftp:

To copy a new configuration from an FTP server to another Cisco Unified SIP Proxy location, use the **copy ftp:** command in module EXEC mode.

copy ftp: {nvram:startup-config | running-config | startup-config | system:running-config}

Syntax Description

nvram:startup-config	Copies the new configuration to the NVRAM saved configuration.
running-config	Copies the new configuration to the current running configuration.
startup-config	Copies the new configuration to the startup configuration in flash memory.
system:running-config	Copies the new configuration to the system configuration.

Command Modes

Module EXEC (>)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

When you copy from the FTP server, the **copy ftp:** command becomes interactive and prompts you for the necessary information.

You may add a username and password to the server IP address if your server is not configured to accept anonymous FTP input. The format would be: *userid:password@ftp-server-address/directory*.

If you do not specify a *directory* value, the software uses the default FTP directory.

The **copy ftp:** command does not copy Cisco Unified SIP Proxy related configuration. To copy Cisco Unified SIP Proxy configurations use the **copy ftp: configuration active** command.

Examples

The following example shows copying the configuration file named start from the FTP server in the default directory to the startup configuration in NVRAM:

```
se-10-0-0-0# copy ftp: nvram:startup-config
Address or name of remote host []? admin:voice@10.3.61.16
Source filename []? start
```

In the following example, the file named start in the FTP server configs directory is copied to the startup configuration:

```
se-10-0-0-0# copy ftp: startup-config
!!!WARNING!!! This operation will overwrite your startup configuration.
Do you wish to continue[y]? y
Address or name of remote host? admin:voice@10.3.61.16/configs
Source filename? start
```

 **copy ftp:**

Related Commands	Command	Description
	copy ftp: configuration active	Copies a new Cisco Unified SIP Proxy configuration from an FTP server to another Cisco Unified SIP Proxy location.
	write	Copies the running configuration to the startup configuration.

copy ftp: configuration active

To copy a new Cisco Unified SIP Proxy configuration from an FTP server to another Cisco Unified SIP Proxy location, use the **copy ftp: configuration active** command in Cisco Unified SIP Proxy EXEC mode.

copy ftp: configuration active

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco Unified SIP Proxy EXEC (cusp)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

When you copy from the FTP server, the **copy ftp: configuration active** command becomes interactive and prompts you for the necessary information.

You may add a username and password to the server IP address if your server is not configured to accept anonymous FTP input. The format would be: *userid:password@ftp-server-address/directory*.

If you do not specify a *directory* value, the software uses the default FTP directory.

Examples

The following example shows copying the configuration file named start from the FTP server in the default directory to the startup configuration in NVRAM:

```
se-10-0-0-0# copy ftp: nvram:startup-config
Address or name of remote host []? admin:voice@10.3.61.16
Source filename []? start
```

Related Commands

Command	Description
copy ftp:	Copies a new configuration from an FTP server to another Cisco Unified SIP Proxy location.

hostname

To configure a hostname for the application that is different from the name used for the host, use the **hostname** command in Cisco Unified SIP Proxy application service configuration mode. To disable the hostname for the application, use the **no** form of this command.

hostname *name*

no hostname *name*

Syntax Description

<i>name</i>	Hostname for the application.
-------------	-------------------------------

Defaults

Hostname configured on the host side.

Command Default

None

Command Modes

Cisco Unified SIP Proxy application service configuration.

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

This command configures the hostname for the application, if it is different from the hostname configured for the Cisco Unified SIP Proxy host. The hostname is limited to 32 characters.

The following error message appears if more than 32 characters are entered:

```
hostname size greater than 32
```

This command modifies configuration directives in */etc/hosts*. It updates the hostname of the hostname-ip mapping entry. If the */etc/hosts* file does not exist, this command creates the */etc/hosts* file and adds an entry in the file. If an application package already has its own bundled */etc/hosts*, the new entries are appended to the existing ones and the original entries remain intact.


Examples

The following example shows two entries in file *etc/hosts*:

```
etc/hosts:
127.0.0.1 localhost.localdomain    localhost ## added by cli
ipaddr   hostname.domain           hostname ## added by cli
```

The IP address, *ipaddr* in the */etc/hosts* file is modified when you use the **bind interface** command.

The first binding of the interface provides the *ipaddr*. For example, if interface *eth0* is bound to each virtual instance by default, *ipaddr* is normally *eth0*. Use the **bind interface** command for multiple bindings.

 hostname**Related Commands**

Command	Description
bind interface	Attaches a device to the application environment.

interface gigabitethernet

To create virtual interfaces for the Cisco Unified SIP Proxy module, use the **interface gigabitethernet** command in module configuration mode. To remove virtual interfaces, use the **no** form of this command.

```
interface gigabitethernet interface.vid

no interface gigabitethernet interface.vid
```

Syntax Description	<i>interface</i>	Physical interface.
	<i>vid</i>	VLAN ID. Valid values are 0 to 4094. For example, gig 0.345 is on VLAN 345.

Command Default No interfaces are created.

Command Modes Module configuration (config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Up to 8 virtual interfaces can be created for each physical interface.

Examples

The following example creates a virtual interface:

```
se-10-0-0-0# configure terminal
se-10-0-0-0(config)# interface gigabitethernet 0.1
```

The following example removes a virtual interface:

```
se-10-0-0-0# configure terminal
se-10-0-0-0(config)# no interface gigabitethernet 0.1
```

ip address

To configure the IP address for a network interface, use the **ip address** command in module interface configuration mode. To remove the IP address interface configuration, use the **no** form of this command.

ip address *ip-address subnet-mask*

no ip address *ip-address subnet-mask*

Syntax Description	<i>ip-address</i>	Configures the IP address.
	<i>subnet-mask</i>	Configures the subnet mask.
Command Default	None	
Command Modes	Module interface configuration (config-subif)	
Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.
Usage Guidelines	Use this command to configure the IP address and network mask for the specified network interface. Changing the IP address for a bound interface results in a message warning the user that the application is bound to the interface. To remove the old IP configuration, reset the virtual instance.	
Examples	<p>The following example sets the IP address of the Gigabit Ethernet interface 0.1:</p> <pre>se-10-0-0-0# configure terminal se-10-0-0-0(config)# interface gigabitethernet 0.1 se-10-0-0-0(config-subif)# ip address 1.1.1.1 255.255.255.0</pre>	
Related Commands	Command	Description
	interface gigabitethernet	Creates virtual interfaces for the Cisco Unified SIP Proxy module.

ip broadcast-address

To define a broadcast address for an interface, use the **ip broadcast-address** command in module interface configuration mode. To restore the default IP broadcast address, use the **no** form of this command.

ip broadcast-address *ip-address*

no ip broadcast-address *ip-address*

Syntax Description	<i>ip-address</i>	IP broadcast address for a network.
Command Default	Default address: 255.255.255.255 (all ones)	
Command Modes	Module interface configuration (config-subif)	
Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples

The following example specifies an IP broadcast address of 0.0.0.0:

```
se-10-0-0-0# configure terminal
se-10-0-0-0(config)# interface gigabitethernet 0.1
se-10-0-0-0(config-subif)# ip broadcast-address 0.0.0.0
```

ip tcp keepalive-time

To configure the amount of idle time that is allowed to pass before sending a keepalive probe, use the **ip tcp keepalive-time** command in module configuration mode. To return to the default value, use the **no** form of this command.

ip tcp keepalive-time *seconds*

no ip tcp keepalive-time *seconds*

Syntax Description	<i>seconds</i>	Time in seconds.
Command Default	7200 seconds	
Command Modes	Module configuration (config)	
Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples

The following example sets the keepalive time to 2000 seconds:

```
se-10-0-0-0# configure terminal
se-10-0-0-0(config)# ip tcp keepalive-time 2000
```

The following example sets the keepalive time to the default value, 7200 seconds:

```
se-10-0-0-0# configure terminal
se-10-0-0-0(config)# no ip tcp keepalive-time
```

log console

To configure the types of messages to be displayed on the console, use the **log console** command in module configuration mode. To stop messages from displaying, use the **no** form of this command.

log console {errors | info | warning}

no log console {errors | info | warning}



Caution

This command generates many screen messages that scroll down the screen until you turn off the display. Seeing the prompt to turn off the display might be difficult. Pressing CTRL-c does not work for this command.

Syntax Description

errors	Error messages.
info	Information messages.
warning	Warning messages.

Command Default

Only fatal error messages are displayed.

Command Modes

Module configuration (config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Because the messages on the console display are also saved in the messages.log file you can use these messages for debugging purposes.

Examples

The following example configures error messages to be displayed on the console:

```
se-10-0-0-0# configure terminal
se-10-0-0-0(config)# log console errors
se-10-0-0-0(config)# exit
```

Related Commands

Command	Description
show logging	Displays the types of messages that are displayed on the console.

log console monitor

To display system messages on the console, use the **log console monitor** command in module EXEC mode. To stop messages from displaying, use the **no** form of this command.

log console monitor {*module* | *entity* | *activity*}

no log console monitor {*module* | *entity* | *activity*}



Caution

This command generates many screen messages that scroll down the screen until you turn off the display. Seeing the prompt to turn off the display might be difficult. Pressing CTRL-c does not work for this command.

Syntax Description

<i>module</i>	Cisco Unified SIP Proxy modules.
<i>entity</i>	Cisco Unified SIP Proxy module entities.
<i>activity</i>	Cisco Unified SIP Proxy entity actions.

Command Default

Only fatal error messages are displayed.

Command Modes

Module EXEC (>)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Because the messages on the console monitor are also saved in the messages.log file you can use these messages for debugging purposes.

Examples

The following example displays messages for results of the database entity in the networking module:

```
se-10-0-0-0# log console monitor networking database results
```

Related Commands

Command	Description
show logging	Displays the types of messages that are displayed on the console.

log server

To configure an external server for saving log messages, use the **log server** command in module configuration mode. To delete the log server, use the **no** form of this command.

log server address {*ip-address* | *hostname*}

no log server address {*ip-address* | *hostname*}

Syntax Description

address <i>ip-address</i>	IP address of the external log server.
address <i>hostname</i>	Hostname of the external log server.

Command Default

No external log server is configured. The local hard disk is used for saving log messages.

Command Modes

Module configuration (config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

An external log server contains a copy of the messages.log file that is stored on the hard disk of the router that contains the Cisco Unified SIP Proxy module. Copying the file to a server permits flexibility in viewing, printing, and troubleshooting system messages.

Examples

The following example assigns 10.1.61.16 as the external log server:

```
se-10-0-0-0# configure terminal
se-10-0-0-0(config)# log server address 10.1.61.16
se-10-0-0-0(config)# exit
```

Related Commands

Command	Description
hostname	Specifies the server that stores the Cisco Unified SIP Proxy applications.
ntp server	Specifies the NTP clocking server.
show hosts	Displays all configured hosts.

log trace boot

To save the trace configuration on rebooting, use the **log trace boot** command in module EXEC mode.

log trace boot

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines The current trace configuration is lost on reboot because tracing is CPU intensive. To ensure that the current trace configuration is saved when the module is rebooted, use the **log trace boot** command.

Examples The following example illustrates the **log trace boot** command:

```
se-10-0-0-0# log trace boot
```

Related Commands	Command	Description
	show trace	Displays the modules and entities being traced.

log trace buffer save

To save the current trace information, use the **log trace buffer save** command in module EXEC mode. To turn off the log trace, use the **no** form of this command.

log trace buffer save

no log trace buffer

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Current trace information stored in the memory buffer can be saved to a file. The file created with the **log trace buffer save** command is atrace_save.log.

Examples The following example illustrates the **log trace buffer save** command:

```
se-10-0-0-0# log trace buffer save
```

Related Commands	Command	Description
	show logs	Displays a list of the trace logs.
	show trace buffer	Displays the modules and entities being traced.

ntp server

To synchronize the Cisco Unified SIP Proxy application system clock with a remote Network Time Protocol (NTP) server, use the **ntp server** command in module configuration mode. To disable the Cisco Unified SIP Proxy application system clock from being synchronized with an NTP server, use the **no** form of this command.

ntp server {*hostname* | *ip-address*} [**prefer**]

no ntp server {*hostname* | *ip-address*}

Syntax Description

<i>hostname</i>	Hostname of the NTP server.
<i>ip-address</i>	IP address of the NTP server.
prefer	(Optional) Marks the server as preferred.

Command Default

The default is the IP address of the server.

Command Default

None

Command Modes

Module configuration (config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command in conjunction with the **clock timezone** command to set the timing functions for Cisco Unified SIP Proxy systems and applications.

The **prefer** option indicates that the specified server is chosen for synchronization from among a set of correctly operating hosts.



Caution

The **no ntp server** command deletes the NTP server hostname or IP address. Use this command with caution.

Examples

The following example assigns the server with address 192.168.1.100 as the preferred NTP server:

```
se-10-0-0-0(config)> ntp server 192.168.1.100 prefer
```

The following example assigns the server with hostname main_ntp as the NTP server:

```
se-10-0-0-0(config)> ntp server main_ntp
```

Related Commands	Command	Description
	clock timezone	Configures the local time zone.
	show clock detail	Displays current clock statistics.
	show ntp source	Displays current NTP server statistics.

offline

To enter the environment for the backup and restore procedures, use the **offline** command in module EXEC mode.

offline

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Default	None
------------------------	------

Command Modes	Module EXEC (>)
----------------------	-----------------

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines	<p>Backup and restore procedures require that you backup your current active configuration using write command if you are going offline to do backup. The offline command disables management interfaces.</p> <p>The offline command does not start the backup or restore procedure. Use the backup and restore commands to initiate those procedures.</p>
-------------------------	---

Examples	The following example illustrates the use of the offline command:
-----------------	--

```
se-9-41-12-28# offline
!!!WARNING!!!: If you are going offline to do a backup, it is recommended
that you save the current running configuration using the 'write' command,
prior to going to the offline state.
```

```
Putting the system offline will disable management interfaces.
```

```
Are you sure you want to go offline? [confirm]
se-9-41-12-28 (offline)#
```

Related Commands	Command	Description
	backup	Selects data to back up and initiates the backup process.
	continue	Exists offline mode and returns to module EXEC mode.
	restore	Selects data to restore and initiates the restore process.

process cpu threshold type

To define the rising and falling threshold values of CPU utilization traps, use the **process cpu threshold type** command.

process cpu threshold type total rising *percentage interval seconds* falling *percentage interval seconds*

Syntax Description

<i>percentage</i>	Defines the rising threshold and the falling threshold in percentage.
<i>seconds</i>	Defines the interval for which the rising and falling threshold values are computed. The range for the interval is 5 to 86,400 seconds.

Command Default

None

Command Modes

Module EXEC (>)

Command History

Cisco Unified SIP Proxy Version	Modification
9.1	This command was introduced.

Usage Guidelines

Backup and restore procedures require that you backup your current active configuration using **write** command if you are going offline to do backup. The **offline** command disables management interfaces.

The **offline** command does not start the backup or restore procedure. Use the **backup** and **restore** commands to initiate those procedures.

Examples

The following example illustrates the use of the **offline** command:

```
se-9-41-12-28# offline
!!!WARNING!!!: If you are going offline to do a backup, it is recommended
that you save the current running configuration using the 'write' command,
prior to going to the offline state.
```

Putting the system offline will disable management interfaces.

```
Are you sure you want to go offline? [confirm]
se-9-41-12-28(offline)#
```


reload

To restart the Cisco Unified SIP Proxy system, use the **reload** command in module offline mode.

reload

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Default	None
------------------------	------

Command Modes	Module offline (offline)
----------------------	--------------------------

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines	Use this command in the following situations:
-------------------------	---

- After a **shutdown** command to restart the Cisco Unified SIP Proxy system.
- After a **restore** command to activate the uploaded file information.

Examples	The following example illustrates the use of the reload command after a restore procedure:
-----------------	---

```
se-10-0-0-0# offline
se-10-0-0-0(offline)# restore id data3 category data
se-10-0-0-0(offline)# reload
```

Related Commands	Command	Description
	backup	Backs up system and application data to a backup server.
	continue	Exits offline mode and returns to Cisco Unified SIP Proxy EXEC mode.
	offline	Switches the Cisco Unified SIP Proxy system to offline mode.
	restore	Restores backup files from the backup server.

restore

To restore a backup file, use the **restore** command in module offline mode.

restore id *backup-id* **category** { **all** | **configuration** | **data** }

Syntax Description

id <i>backup-id</i>	Specifies the ID number of the file to be restored.
category	Precedes the name of the file type to be restored.
all	Specifies that the file to be restored contains system and application settings, application data, and voice messages.
configuration	Specifies that the file to be restored contains only system and application settings.
data	Specifies that the file to be restored contains only application data and voice messages.

Command Default

The backup file is not restored.

Command Modes

Module offline (offline)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

When the restore procedure begins, all active calls are terminated. Cisco Unified SIP Proxy does not support scheduled restores. Consider restoring a file when the phones are least active.

After completing the restore procedure, use the **reload** command to activate the file data.

Use the **show backup history** command to locate the *backup-id* value of the file to be restored.

Examples

The following example restores the file with the ID data5, which is a data-only file.

```
se-10-0-0-0> enable
se-10-0-0-0# offline
se-10-0-0-0(offline)# restore id data5 category data
se-10-0-0-0(offline)# reload
```

Related Commands

Command	Description
continue	Exits offline mode and returns to module EXEC mode.
offline	Enters offline mode.
reload	Restarts the Cisco Unified SIP Proxy system.

■ restore

Command	Description
show backup history	Displays the status of backup procedures.
show backup server	Displays the network FTP server designated as the backup server.

restore factory default

To restore the system to the factory defaults, use the **restore factory default** command in module offline mode.

restore factory default


Caution

This feature is not reversible. All data and configuration files are erased. Use this feature with caution. We recommend that you do a full system backup before proceeding with this feature.

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Module offline (offline)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines

Restoring the system to the factory defaults has the following effects:

- Replaces the current database with an empty database.
- Initializes Lightweight Directory Access Protocol (LDAP) to an empty state.
- Replaces the startup configuration with the template startup configuration that ships with the system.
- Erases all postinstallation configuration data.
- Deletes all subscriber and custom prompts.

When the system is clean, the administrator sees a message that the system will reload, and the system begins to reload. When the reload is complete, the system prompts the administrator to go through the postinstallation process.

Examples

The following example restores the system to factory defaults.

- Step 1

Put the system into offline mode.

se-10-0-0-0# **offline**
- Step 2

Restore the system to factory defaults.

se-10-0-0-0 (offline)# **restore factory default**

restore factory default

This operation will cause all the configuration and data on the system to be erased. This operation is not reversible. Do you wish to continue? (n)

Step 3 Do one of the following:

- Enter **n** to retain the system configuration and data.
The operation is canceled, and the system remains in offline mode. To return to online mode, enter **continue**.
- Enter **y** to erase the system configuration and data.
When the system is clean, a message appears indicating that the system will start to reload. When the reload is complete, a prompt appears to start the postinstallation process.

Related Commands

Command	Description
continue	Returns to Cisco Unified SIP Proxy online mode.
offline	Enters Cisco Unified SIP Proxy offline mode.

security ssh known-hosts

To configure the MD5 (Message-Digest algorithm 5) fingerprint and type of host key for the SSH (Secure Shell) server's host key, use the **security ssh known-hosts** command in module configuration mode. Use the **no** form of this command to remove the MD5 fingerprint.

security ssh known-hosts *host* {**ssh-rsa** | **ssh-dsa**} *fingerprint-string*

no security ssh known-hosts *host* {**ssh-rsa** | **ssh-dsa**} *fingerprint-string*

Syntax Description

<i>host</i>	Hostname or IP address of the SSH server.
<i>ssh-rsa</i>	The RSA encryption algorithm was used to create this fingerprint for an SSH server's host key.
<i>ssh-dsa</i>	The DSA (Digital Signature Algorithm) was used to create this fingerprint for an SSH server's host key.
<i>fingerprint-string</i>	MD5 fingerprint string.

Command Default

No server authentication performed for the specified host.

Command Modes

Module configuration (config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use the **security ssh known-hosts** command in Cisco Unified SIP Proxy EXEC mode to configure the MD5 fingerprint of the SSH server's host key. When the fingerprint is configured, the local SSH/FTP client performs server authentication by comparing the configured fingerprint with the one returned from the SSH server.

The *host* argument can be either a hostname or a IP address.

If the fingerprint is not configured, no server authentication is performed. The fingerprint is not saved in the startup configuration when you use the **write** command.

Examples

The following example specifies the MD5 fingerprint of a SSH-RSA server's host key:

```
se-10-0-0-0# configure terminal
se-10-0-0-0(config)# security ssh known-hosts server.example.com ssh-rsa
a5:3a:12:6d:e9:48:a3:34:be:8f:ee:50:30:e5:e6:c3
```

Related Commands	Command	Description
	backup server authenticate	Retrieves the fingerprint of the backup server's host key.
	show security ssh	Displays a list of configured SSH servers and their fingerprints.
	write	Copies the running configuration to the startup configuration.

show backup

To display information about the server that is used to store backup files, use the **show backup** command in module EXEC mode.

show backup

Syntax Description This command has no arguments or keywords.

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines This command displays the FTP server URL, the subscriber account on the FTP server, and the number of backup file revisions that are to be stored on the server.

Examples The following is sample output from the **show backup** command:

```
se-10-0-0-0> show backup
```

```
Server URL:                               ftp://10.12.0.1/ftp
User Account on Server:
Number of Backups to Retain:              5
```

[Table 1](#) describes the significant fields shown in the display.

Table 1 *show backup Field Descriptions*

Field	Description
Server URL	IP address of the backup server.
User Account on Server	(Optional) User ID on the backup server.
Number of Backups to Retain	Number of backup files to store before the oldest one is overwritten.

Related Commands	Command	Description
	backup	Selects the backup data and initiates the backup process.

show backup history

To display the success or failure of backup and restore procedures, use the **show backup history** command in module EXEC mode.

show backup history

Syntax Description This command has no arguments or keywords.

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines This command displays each backup file, its backup ID, the type of data stored in the file, and the success or failure of the backup procedure.

Examples The following is sample output from the **show backup history** command:

```
se-10-0-0-0> show backup history

blade522> show backup history
#Start Operation
Category:      Configuration
Backup Server: ftp://192.168.1.35/pub/cusp_backup
Operation:     Backup
Backupid:      1
Date:          Tue Oct 21 06:14:30 EDT 2008
Result:        Success
Reason:
#End Operation

#Start Operation
Category:      Configuration
Backup Server: ftp://192.168.1.35/pub/cusp_backup
Operation:     Restore
Backupid:      1
Restoreid:     1
Date:          Tue Oct 21 06:17:21 EDT 2008
Result:        Success
Reason:
#End Operation
```

[Table 2](#) describes the significant fields shown in the display.

Table 2 *show backup history Field Descriptions*

Field	Description
Category	Specifies the type of file (data, configuration, or all) that was backed up.
Backup Server	Backup server location.
Operation	Type of operation performed.
Backupid	ID number of the backup file.
Restoreid	ID to use to restore this file.
Description	Optional description of the backup procedure.
Date	Date and time (in hh:mm:ss) when the operation occurred.
Result	Indication of success or failure of the operation.
Reason	If the operation failed, this field gives the reason for the failure.

Related Commands

Command	Description
backup	Selects the backup data and initiates the backup process.
show backup server	Displays the backup file ID.

show backup server

To display the details of the most recent backup files, use the **show backup server** command in module EXEC mode.

show backup server

Syntax Description This command has no arguments or keywords.

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use this command to display a list of the backup files available on the backup server. The files are grouped by category, with the date of each backup and the backup file ID. For information on the success or failure of a backup procedure, see the [show backup history](#) command.

Examples The following is sample output for the **show backup server** command:

```
se-10-0-0-0> show backup server

Category:      Data
Details of last 5 backups
Backupid:      1
Date:          Tue Jul 22 10:55:52 PDT 2008
Description:

Backupid:      2
Date:          Tue Jul 29 18:06:33 PDT 2008
Description:

Backupid:      3
Date:          Tue Jul 29 19:10:32 PDT 2008
Description:

Category:      Configuration
Details of last 5 backups
Backupid:      1
Date:          Tue Jul 22 10:55:48 PDT 2008
Description:

Backupid:      2
Date:          Tue Jul 29 18:06:27 PDT 2008
Description:

Backupid:      3
Date:          Tue Jul 29 19:10:29 PDT 2008
```

show backup server

Description:

Table 3 describes the significant fields shown in the display.

Table 3 *show backup server Field Descriptions*

Field	Description
Category	Type of backup file.
Backupid	ID number of the backup file.
Date	Date and time (in hh:mm:ss) when the file was backed up.
Description	Optional description of the backup file.

Related Commands

Command	Description
backup	Selects the backup data and initiates the backup process.
show backup history	Displays the success or failure of backup and restore procedures.

show clock detail

To display clock statistics, use the **show clock detail** command in module EXEC mode.

show clock detail

Syntax Description This command has no arguments or keywords.

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples In the following example, the clock statistics are displayed on the screen.

```
se-100.0.4.2> show clock detail
se-10-1-1-20> show clock detail
15:22:08.375 PST Thu Nov 29 2007
time zone:                      America/Los_Angeles
clock state:                     unsync
delta from reference (microsec): 0
estimated error (microsec):      16
time resolution (microsec):      1
clock interrupt period (microsec): 10000
time of day (sec):                1196378528
time of day (microsec):           378926
```

Related Commands	Command	Description
	clock timezone	Configures the local time zone.
	ntp server	Configures the NTP server for time synchronization.

show interfaces

To display all the configured interfaces, including virtual and VLAN interfaces, use the **show interfaces** command in module EXEC mode.

show interfaces [**|** **GigabitEthernet** **| ide**]

Syntax Description		Pipes output to another command.
	GigabitEthernet	Gigabit Ethernet device.
	ide	Integrated Drive Electronics (hard disk)

Command Modes	Module EXEC (>)
---------------	-----------------

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples In the following example, the **show interfaces** command displays all configured interfaces on the screen: a Gigabit Ethernet interface and an IDE (hard disk) interface.

```
se-100.0.4.2> show interfaces
GigabitEthernet 0 is up, line protocol is up
  Internet address is 10.10.1.20 mask 255.255.255.0 (configured on router)
    25629 packets input, 1688582 bytes
    0 input errors, 0 dropped, 0 overrun, 0 frame errors
    25634 packets output, 1785015 bytes
    0 output errors, 0 dropped, 0 overrun, 0 collision errors
    0 output carrier detect errors

IDE hd0 is up, line protocol is up
  2060 reads, 32704512 bytes
  0 read errors
  489797 write, 2520530944 bytes
  0 write errors
```

Related Commands	Command	Description
	show running-config	Displays the current running configuration.

show logs

To display a list of system logs, use the **show logs** command in module EXEC mode.

show logs

Syntax Description This command has no arguments or keywords.

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use this command to display all the log files under the /var/log directory of the virtual instance.

Examples In the following example, the **show logs** command shows the log files under the /var/log directory of the virtual instance.

```
se-Module(exec-mping)> show logs
SIZE                LAST_MODIFIED_TIME                NAME
28719  Mon Dec 22 14:15:06 EST 2008  linux_session.log
2573   Fri Dec 19 08:28:13 EST 2008  install.log
8117   Fri Dec 19 08:27:51 EST 2008  dmesg
2274   Fri Dec 19 08:27:55 EST 2008  syslog.log
10455  Thu Dec 18 16:38:13 EST 2008  sshd.log.prev
1268   Fri Dec 19 08:28:09 EST 2008  atrace.log
384    Fri Dec 19 08:27:55 EST 2008  debug_server.log
10380  Thu Dec 18 16:06:58 EST 2008  postgres.log.prev
1361   Fri Dec 19 08:28:14 EST 2008  sshd.log
5598   Fri Dec 19 08:30:13 EST 2008  postgres.log
1014   Fri Dec 19 08:27:57 EST 2008  klog.log
2298494 Sun Dec 21 23:30:00 EST 2008  messages.log
85292  Fri Dec 19 08:25:33 EST 2008  shutdown_installer.log
```

show ntp associations

To display the association identifier and status for all Network Time Protocol (NTP) servers, use the **show ntp associations** command in module EXEC mode.

show ntp associations [**assocID** *association-id*]

Syntax Description	assocID <i>association-id</i>	Specified association ID.
---------------------------	--------------------------------------	---------------------------

Command Modes	Module EXEC (>)
----------------------	-----------------

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use the **show ntp associations** command to display the association identifier and status for all the NTP servers configured for Cisco Unified SIP Proxy and not details about the servers. The **show ntp associations assocID association-id** command provides details on the status of a specified NTP server.

Use the status field to determine the configuration and status of all the NTP servers. This field consists of 4 hexadecimal digits:

- The first two digits specify the server configuration and how far it progressed through the clock selection process. See [Table 4](#).
- The second two digits indicate the number of events and the type of the last event. See [Table 5 on page 49](#).

[Table 4](#) shows common status codes and their descriptions. The first digit specifies the configuration, reachability, and authentication status for the specified server. The second digit records how well the specified server passed through the clock selection algorithm.

Table 4 Status Field Code Descriptions

Status Field Codes	Description
1xxx	Server has sent a peer synchronization request to the local machine, and the server is not configured locally.
7xxx	Server is a peer that is not configured locally and is reachable and using proper authentication.
8xxx	Server is configured and not authenticated or reachable.
9xxx	Server is configured and reachable.
Cxxx	Server is configured to use authentication and is not reachable.
Dxxx	Server is configured to use authentication and is reachable; it is not using a trusted key.
Fxxx	Server is authenticated as a trusted server and is reachable.

Table 4 Status Field Code Descriptions (continued)

Status Field Codes	Description
x0xx	Server did not pass any sanity checks and is rejected by the client. Possible causes for this condition include the server failing to authenticate, the server having a huge error bound (over 16 seconds), or the server existing on a higher stratum number than the client.
x1xx	Server passed the sanity checks and was not close enough to other servers to survive the intersection algorithm. This indicates that the server's clock was outside the largest possible error bounds of the other clocks, a condition that usually indicates that the server is set to the wrong time.
x2xx	Server passed the correctness checks (intersection algorithm). This value indicates that the server is probably configured correctly.
x3xx	Server passed the candidate checks. The server was not discarded because there were too many good servers (over 10).
x4xx	Server passed through the clustering algorithms without being discarded as an outlier having too much dispersion.
x5xx	Server would be the synchronization source and is too far away. This means that all the other clocks did not pass the sanity check or are also too far away.
x6xx	Server is the current synchronization source. This is the preferred server status.
x7xx to xFxx	Reserved values. These should not occur in normal usage.

Table 5 lists the event codes. The third digit indicates the number of events that occurred since the last time an error was returned to the console by NTP or by one of the **show ntp** commands. This value does not wrap and stops incrementing at 15 (or hex F).

For a properly running server, the value should be xx1x, unless one of the **show ntp** commands has queried the server since startup. In that case, the value should be xx0x. If the third digit is any other value, check for the event causing errors.

The fourth digit in the field indicates the last event that occurred. For properly running servers, the event should be the server becoming reachable.

Table 5 Event Field Code Values

Event Field Codes	Description
xxx0	Unspecified event. Either no events have occurred or a special error has occurred.
xxx1	IP error occurred reaching the server.
xxx2	Unable to authenticate a server that used to be reachable. This indicates that the keys changed or someone is spoofing the server.
xxx3	Formerly reachable server is now unreachable.
xxx4	Formerly unreachable server is now reachable.

Table 5 Event Field Code Values (continued)

Event Field Codes	Description
xxx5	Server's clock had an error.
xxx6 to xxxF	Reserved values. These should not occur in normal usage.

The flash field indicates the status of the packets while a series of 12 diagnostic tests are performed on them. The tests are performed in a specified sequence to gain maximum information while protecting against accidental or malicious errors.

The flash variable is set to zero as each packet is received. If any bits are set as a result of the tests, the packet is discarded.

The tests look for the following information:

- TEST1 to TEST3 check the packet time stamps from which the offset and delay are calculated. If no bits are set, the packet header variables are saved.
- TEST4 and TEST5 check access control and cryptographic authentication. If no bits are set, no values are saved.
- TEST6 to TEST8 check the health of the server. If no bits are set, the offset and delay relative to the server are calculated and saved.
- TEST9 checks the health of the association. If no bits are set, the saved variables are passed to the clock filter and mitigation algorithm.
- TEST10 to TEST12 check the authentication state using Autokey public-key cryptography. If any bits are set and the association was previously marked as reachable, the packet is discarded. Otherwise, the originate and receive time stamps are saved with a continuation of the process.

Table 6 lists the flash bits for each test.

Table 6 Flash Field Diagnostic Bit Values

Flash Bit Values	Description
0x001	TEST1. Duplicate packet. The packet is at best a casual retransmission and at worst a malicious replay.
0x002	TEST2. Bogus packet. The packet is not a reply to a message previously sent. This can happen when the NTP daemon is restarted.
0x004	TEST3. Unsynchronized. One or more time-stamp fields are invalid. This normally happens when the first packet from a peer is received.
0x008	TEST4. Access is denied.
0x010	TEST5. Cryptographic authentication fails.
0x020	TEST6. Server is unsynchronized. Wind up its clock first.
0x040	TEST7. Server stratum is at the maximum of 15. The server is probably unsynchronized, and its clock needs to be wound up.
0x080	TEST8. Either the root delay or the dispersion is greater than 1 second.
0x100	TEST9. Either the peer delay or the dispersion is greater than 1 second.

Table 6 Flash Field Diagnostic Bit Values (continued)

Flash Bit Values	Description
0x200	TEST10. Autokey protocol detected an authentication failure.
0x400	TEST11. Autokey protocol did not verify the server, or the peer is proventic and has valid key credentials.
0x800	TEST12. Protocol or configuration error occurred in the public key algorithm, or a possible intrusion event is detected.

Examples

The following example show the output that appears after using the basic **show ntp associations** command:

```
se-10-0-0-0> show ntp associations
```

```
ind assID status conf reach auth condition last_event cnt
=====
1 50101 8000 yes yes none sys.peer reachable 2
```

[Table 7](#) describes the significant fields shown in the display.

Table 7 show ntp associations Field Descriptions

Field	Description
ind	Index number of the association.
assID	Peer identifier returned by the server.
status	Hexadecimal value of the server status. See Table 4 on page 48 and Table 5 on page 49 for a description of these field codes.
conf	Indicates whether the server is configured or not. Valid values are yes and no.
reach	Indicates whether the peer is reachable or not. Valid values are yes and no.
auth	Status of the server authentication. Valid values are: <ul style="list-style-type: none"> ok bad none “ ”

Table 7 *show ntp associations Field Descriptions (continued)*

Field	Description
condition	Type of association in the clock selection process. Valid values are: <ul style="list-style-type: none"> space: Reject. Peer is discarded as unreachable. false-tick: Peer is discarded as a false tick. excess: Peer is discarded as not among the 10 closest peers. outlier: Peer is discarded as an outlier. candidate: Peer selected for possible synchronization. selected: Almost synchronized to this peer. sys.peer: Synchronized to this peer. pps.peer: Synchronized to this peer on the basis of a pulse-per-second signal.
last_event	Last event that occurred in the system. Valid values are: <ul style="list-style-type: none"> (empty) IP error Auth fail lost reach reachable clock expt See Table 5 for descriptions of these values.
cnt	Number of events that occurred since the last time an error was returned to the console by the NTP. This value does not wrap and stops incrementing at 15 (or hex F). For a properly functioning server, this value must be 1 or 0.

The following example shows the ntp associations for a particular assocID, using the **show ntp associations assocID** command:

```
se-10-0-0-0> show ntp associations assocID 50101
```

```
status=8000 unreach, conf, no events,
srcadr=10.1.10.2, srcport=123, dstadr=10.1.1.20, dstport=123, leap=11,
stratum=16, precision=-17, rootdelay=0.000, rootdispersion=0.000,
refid=0.0.0.0, reach=000, unreach=16, hmode=3, pmode=0, hpoll=10,
ppoll=10, flash=00 ok, keyid=0, offset=0.000, delay=0.000,
dispersion=0.000, jitter=4000.000,
reftime=00000000.00000000 Wed, Feb  6 2036 22:28:16.000,
org=00000000.00000000 Wed, Feb  6 2036 22:28:16.000,
rec=00000000.00000000 Wed, Feb  6 2036 22:28:16.000,
xmt=cafae952.b5de7a74 Fri, Nov 30 2007 11:56:02.710,
filtdelay=    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00,
filtoffset=   0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00,
filtdisp=  16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0
```

[Table 8](#) describes the significant fields shown in the display.

Table 8 *show ntp associations assocID Field Descriptions*

Field	Description
status	Status of the peer. See Table 4 on page 48 , Table 5 on page 49 , and Table 7 on page 51 for descriptions of the values in this line.
srcadr	IP address of the host server.
srcport	Port address of the host server.
dstadr	IP address of the destination server.
dstport	Port address of the destination server.
leap	Two-bit coded warning of an impending leap second to be inserted in the NTP timescale. Valid values are: <ul style="list-style-type: none"> • 00: No warning • 01: Last minute has 61 seconds • 10: Last minute has 59 seconds • 11: Alarm condition (clock not synchronized)
stratum	Server hop count to the primary clock source. Valid values are: <ul style="list-style-type: none"> • 0: Unspecified • 1: Primary clock reference • 2–255: Secondary reference via NTP If the stratum value is 15, the server is probably unsynchronized and its clock needs to be reset.
precision	Precision of the clock, in seconds to the power of two.
rootdelay	Total round-trip delay, in seconds, to the primary reference source at the root of the synchronization subnet.
rootdispersion	Maximum error, in seconds, relative to the primary reference source at the root of the synchronization subnet.
refid	IP address of the peer selected for synchronization.
reach	Peer reachability status history, in octal. Each bit is set to 1 if the server is reached during a polling period and is set to 0 otherwise. The value 377 indicates that the last 8 attempts were good.
unreach	Number of poll intervals since the last valid packet was received.

Table 8 *show ntp associations assocID Field Descriptions (continued)*

Field	Description
hmode	Association mode of the host server. Valid values are: <ul style="list-style-type: none"> • 0: Unspecified • 1: Symmetric active • 2: Symmetric passive • 3: Client • 4: Server • 5: Broadcast • 6: Reserved for NTP control messages • 7: Reserved for private use
pmode	Association mode of the peer server. Valid values are: <ul style="list-style-type: none"> • 0: Unspecified • 1: Symmetric active • 2: Symmetric passive • 3: Client • 4: Server • 5: Broadcast • 6: Reserved for NTP control messages • 7: Reserved for private use
hpoll	Minimum interval, in seconds as a power of two, between transmitted messages from the host.
ppoll	Minimum interval, in seconds as a power of two, between transmitted messages to the peer.
flash	Status of the packet after a series of diagnostic tests are performed on the packet. See the description of the flash field values in Table 5 .
keyid	ID of the cryptographic key used to generate the message-authentication code.
offset	Time difference between the client and the server, in milliseconds.
delay	Round-trip delay of the packet, in milliseconds.
dispersion	Measure, in milliseconds, of how scattered the time offsets are from a specific time server.
jitter	Estimated time error, in milliseconds, of the Cisco Unified SIP Proxy clock measured as an exponential average of RMS time differences.
reftime	Local time, in time-stamp format, when the local clock was last updated. If the local clock was never synchronized, the value is zero.

Table 8 *show ntp associations assocID Field Descriptions (continued)*

Field	Description
org	Local time, in time-stamp format, at the peer when its latest NTP message was sent. If the peer becomes unreachable, the value is zero.
rec	Local time, in time-stamp format, when the latest NTP message from the peer arrived. If the peer becomes unreachable, the value is zero.
xmt	Local time, in time-stamp format, at which the NTP message departed from the sender.
filtdelay	Round-trip delay, in seconds, between the peer clock and the local clock over the network between them.
filtoffset	Offset, in seconds, of the peer clock relative to the local clock.
filtdisp	Maximum error, in seconds, of the peer clock relative to the local clock over the network between them. Only values greater than zero are possible.

Related Commands

Command	Description
show ntp servers	Displays a list of NTP servers and their current states.
show ntp source	Displays the primary time source for an NTP server.

show ntp servers

To display a list of Network Time Protocol (NTP) servers, their current states, and a summary of the remote peers associated with each server, use the **show ntp servers** command in module EXEC mode.

show ntp servers

Syntax Description This command has no keywords or arguments.

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use the **show ntp servers** command after changing the ntp server configuration.

Examples The following example shows sample output for the **show ntp servers** command:

```
se-10-1-1-20> show ntp servers
      remote      refid      st t when poll reach  delay  offset  jitter
=====
 10.1.10.2      0.0.0.0      16 u   - 1024    0   0.000   0.000 4000.00
space reject,      x falsetick,      . excess,      - outlier
+ candidate,      # selected,      * sys.peer,      o pps.peer
```

Table 9 describes the significant fields shown in the display.

Table 9 *show ntp servers Field Descriptions*

Field	Description
remote	IP address of the remote server.
refid	Server's current time source.
st	Hop count (stratum) to the remote server.
t	Type of peer. Valid values are: <ul style="list-style-type: none"> l: Local u: Unicast m: Multicast b: Broadcast
when	Time when the last packet was received.
poll	Polling interval, in seconds.

Table 9 *show ntp servers Field Descriptions (continued)*

Field	Description
reach	Peer reachability status history, in octal. Each bit is set to 1 if the server is reached during a polling period and is set to 0 otherwise. The value 377 indicates that the last 8 attempts were good.
delay	Round-trip delay of the packet, in milliseconds.
offset	Time difference between the client and the server, in milliseconds.
jitter	Estimated time error, in milliseconds, of the Cisco Unified SIP Proxy clock measured as an exponential average of RMS time differences.
(tally code)	<p>The character preceding the remote IP address indicates the status of the association in the clock selection process. Valid values are:</p> <ul style="list-style-type: none"> • space Reject: Peer is discarded as unreachable. • x Falsetick: Peer is discarded as a false tick. • . Excess: Peer is discarded as not among the ten closest peers. • – Outlier: Peer is discarded as an outlier. • + Candidate: Peer selected for possible synchronization. • # Selected: Almost synchronized to this peer. • * Sys.peer: Synchronized to this peer. • o PPS.peer: Synchronized to this peer on the basis of a pulse-per-second signal.

Related Commands

Command	Description
ntp server	Configures the NTP server.
show ntp associations	Displays a list of association identifiers and peer statuses for an NTP server.
show ntp source	Displays the time source for an NTP server.

show ntp source

To display the time source for a Network Time Protocol (NTP) server, use the **show ntp source** command in module EXEC mode. The display extends back to the primary time source, starting from the local host.

show ntp source [detail]

Syntax Description	detail	(Optional) Additional NTP server details including: precision, leap, refit, delay, dispersion, root delay, root dispersion, reference time, originate timestamp, and transmit timestamp.
---------------------------	---------------	--

Command Modes	Module EXEC (>)
----------------------	-----------------

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples The following example shows the sample output for the **show ntp source** command:

```
se-10-0-0-0> show ntp source
```

```
127.0.0.1: stratum 9, offset 0.000015, synch distance 0.03047
10.100.10.65: stratum 8, offset -0.001124, synch distance 0.00003
```

Table 10 describes the significant fields shown in the display.

Table 10 *show ntp source Field Descriptions*

Field	Description
(first field)	IP address of the host.
stratum	Server hop count to the primary clock source. Valid values are: <ul style="list-style-type: none"> 0: Unspecified 1: Primary clock reference 2–255: Secondary reference via NTP
offset	Time offset between the host and the local host, in seconds.
synch distance	Host synchronization distance, which is the estimated error relative to the primary source.

The following example shows the sample output for the **show ntp source detail** command:

```
se-1-100-5-2> show ntp source detail

server 10.0.0.1, port 123
stratum 9, precision -17, leap 00
refid [10.10.10.65] delay 0.00012, dispersion 0.00000 offset 0.000011
rootdelay 0.00058, rootdispersion 0.03111, synch dist 0.03140
reference time:      af4a3ff7.926698bb  Thu, Feb 30 2007 14:47:19.571
originate timestamp: af4a4041.bf991bc5  Thu, Nov 30 2007 14:48:33.748
transmit timestamp:  af4a4041.bf90a782  Thu, Nov 30 2007 14:48:33.748

server 10.10.10.65, port 123
stratum 8, precision -18, leap 00
refid [172.16.7.1] delay 0.00024, dispersion 0.00000 offset -0.001130
rootdelay 0.00000, rootdispersion 0.00003, synch dist 0.00003
reference time:      af4a402e.f46eaea6  Thu, Nov 30 2007 14:48:14.954
originate timestamp: af4a4041.bf6fb4d4  Thu, Nov 30 2007 14:48:33.747
transmit timestamp:  af4a4041.bfb0d51f  Thu, Nov 30 2007 14:48:33.748
```

Table 11 describes the significant fields shown in the display.

Table 11 *show ntp source detail Field Descriptions*

Field	Description
server	IP address of the host server.
port	Port number of the host server.
stratum	Server hop count to the primary clock source. Valid values are: <ul style="list-style-type: none"> 0: Unspecified 1: Primary clock reference 2–255: Secondary reference via NTP
precision	Precision of the clock, in seconds to the power of two.
leap	Two-bit code warning of an impending leap second to be inserted in the NTP time scale. Valid values are: <ul style="list-style-type: none"> 00: No warning 01: Last minute was 61 seconds 10: Last minute was 59 seconds 11: Alarm condition (clock not synchronized)
refid	IP address of the peer selected for synchronization.
delay	Round-trip delay of the packet, in milliseconds.
dispersion	Measure, in milliseconds, of how scattered the time offsets have been from a given time server.
offset	Time offset between the host and the local host, in seconds.
rootdelay	Total round-trip delay, in seconds, to the primary reference source at the root of the synchronization subnet.
rootdispersion	Maximum error, in seconds, relative to the primary reference source at the root of the synchronization subnet.
synch dist	Host synchronization distance, which is the estimated error relative to the primary source.

Table 11 *show ntp source detail Field Descriptions (continued)*

Field	Description
reference time	Local time, in time-stamp format, when the local clock was last updated. If the local clock was never synchronized, the value is zero.
originate timestamp	Local time, in time-stamp format, at the peer when its latest NTP message was sent. If the peer becomes unreachable, the value is zero.
transmit timestamp	Local time, in time-stamp format, when the latest NTP message from the peer arrived. If the peer becomes unreachable, the value is zero.

Related Commands

Command	Description
show ntp associations	Displays a list of association identifiers and peer statuses for an NTP server.
show ntp servers	Displays a list of NTP servers and their current states.

show ntp status

To display statistics for the Network Time Protocol (NTP) server, use the **show ntp status** command in module EXEC mode.

show ntp status

Syntax Description This command has no arguments or keywords.

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples The following is sample output for the **show ntp status** command:

```
se-10-0-0-0> show ntp status
```

```
NTP reference server 1:      10.100.6.9
Status:                     sys.peer
Time difference (secs):     3.268110005008586E8
Time jitter (secs):         0.17168384790420532
```

[Table 12](#) describes the significant fields shown in the display.

Table 12 *show ntp status Field Descriptions*

Field	Description
NTP reference server 1	IP address of the NTP server.
Status	<p>Status of the peer association in the clock selection process. Valid values are:</p> <ul style="list-style-type: none"> Reject: Peer is discarded as unreachable. Falsetick: Peer is discarded as a false tick. Excess: Peer is discarded as not among the ten closest peers. Outlier: Peer is discarded as an outlier. Candidate: Peer selected for possible synchronization. Selected: Almost synchronized to this peer. Sys.peer: Synchronized to this peer. PPS.peer: Synchronized to this peer on the basis of a pulse-per-second signal.

Table 12 *show ntp status Field Descriptions (continued)*

Field	Description
Time difference (secs)	Difference in seconds between the system clock and the NTP server.
Time jitter (secs)	Estimated time error, in seconds, of the Cisco Unified SIP Proxy clock measured as an exponential average of root mean square (RMS) time differences.

Related Commands

Command	Description
clock timezone	Sets the local time zone.
ntp server	Specifies the NTP server for the Cisco Unified SIP Proxy.
show clock detail	Displays clock statistics.

show process

To display all processes in the application environment, use the **show process** command in module EXEC mode.

show process [cpu | memory]

Syntax Description

cpu	Displays Central Processing Unit (CPU) utilization.
memory	Displays Random Access Memory (RAM) utilization.

Command Modes

Module EXEC (>)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to display all processes in the virtual application environment sorted by process ID in ascending order.

Examples

The following example displays CPU utilization:

```
se-Module(exec-mping)> show process cpu
Uptime (secs):          6536.02
User time (secs):       55.93
Kernel time (secs):     4.48
Idle time (secs):       6452.87
```

The following example displays all processes in the virtual application environment:

```
se-192-168-202-102# show process
STATE      HEALTH  CMD
online     alive   syslog-ng
online     alive   platform_config
online     alive   trace
online     alive   rbcpl
online     alive   cli
online     alive   ntp
online     alive   ldap
online     alive   sql
online     alive   downloader
online     alive   http
online     alive   probe
online     alive   mgmt
online     alive   snmp
online     alive   superthread
online     alive   dns
online     alive   backupprestore
online     alive   usermanager
online     alive   nrs
online     alive   config-gw
```

Table 13 *show process Field Descriptions*

Field	Description
Uptime	The number of seconds since the last reboot.
User time	The number of seconds since the last reboot that the system has spent executing nonprivileged code.
Kernel time	The number of seconds since the last reboot that the system has spent executing privileged code.
Idle time	The number of seconds since the last reboot that the system spent idle.
STATE	There are two possible states: <ul style="list-style-type: none"> • online—The subsystem is ready to handle requests. • ready-to-go-online—The subsystem is ready, but the main processing system has not brought the subsystem online.
HEALTH	There are two possible health conditions: <ul style="list-style-type: none"> • alive—The primary thread of the process exists. • dead—The primary thread of the process does not exist. Usually, a dead primary thread will cause the subsystem to restart.
CMD	The name of the subsystem.

Related Commands

Command	Description
show tech-support	Displays a summary of the diagnostic information for the application.

show running-config

To display the committed running configuration of the Cisco Unified SIP Proxy application environment, use the **show running-config** command in Cisco Unified SIP Proxy application service EXEC mode.

show running-config

Syntax Description This command has no arguments or keywords.

Command Modes Cisco Unified SIP Proxy application service EXEC

Command History	Cisco Unified SIP Proxy
Version	Modification
1.0	This command was introduced.

Usage Guidelines For the Cisco Unified SIP Proxy, the running configuration only displays the configuration changes that were committed with the **commit** command.

Examples

```
se-Module(exec-mping)> show running-config
app-service mping
bind interface eth0
hostname se-10-0-0-0
exit
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	show tech-support	Displays a summary of the diagnostic information for the application.

show security ssh known-hosts

To display a list of configured SSH (Secure Shell) servers and their fingerprints, use the **show security ssh known-hosts** command in module EXEC mode.

show security ssh known-hosts

Syntax Description This command has no arguments or keywords.

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use the **show security ssh known-hosts** command in module EXEC mode to display a list of configured SSH servers and their fingerprints. These fingerprints are used to perform SSH server authentication.

Examples The following is sample output for the **show security ssh known-hosts** command:

```
se-10-0-0-0# show security ssh known-hosts

192.168.138.208 ssh-rsa a5:3a:12:6d:e9:48:a3:34:be:8f:ee:50:30:e5:e6:c3
172.16.103.231 ssh-rsa 5c:31:00:89:04:ed:2e:fc:bd:eb:26:23:cd:24:c0:b6
```

This output shows the following information:

- Hostname or IP address of the SSH server.
- Whether the MD5 (Message-Digest algorithm 5) fingerprint is for a SSH server's host key that was created using the DSA (Digital Signature Algorithm) or RSA encryption algorithm.
- MD5 fingerprint string.

Related Commands	Command	Description
	backup server authenticate	Retrieves the fingerprint of the backup server's host key.
	security ssh known-hosts	Configures the MD5 fingerprint of the SSH server's host key.

show software

To display characteristics of the installed software, use the **show software** command in module EXEC mode.

show software {directory | download server | packages | versions}

Syntax Description	dependencies	Displays subsystem dependencies.
	directory	Displays the software directory.
	download server	Displays the IP address of the FTP server.
	packages	Displays the configured Cisco Unified SIP Proxy application packages.
	versions	Displays the current versions of the configured software and applications.

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples The following is sample output for the **show software** command:

```
se-10-0-0-0> show software download server
```

```
Download server URL is: ftp://127.0.0.1/ftp
```

```
se-10-0-0-0> show software packages
```

```
Installed Packages:
```

```
- Installer (Installer application ) (0.0.0.12)
- Bootloader (Primary) (Service Engine Bootloader) (2.1.1.14)
- Infrastructure (Service Engine Infrastructure) (2.3.2.1)
- Global (Global manifest) (0.0.0.12)
- cusp (CUSP subsyste) (1.0.1)
- Bootloader (Secondary) (Service Engine BootLoader) (0.0.0.12)
- Core (Service Engine OS Core) (2.4.0.2)
- GPL Infrastructure (Service Engine GPL Infrastructure) (2.2.1.1)
```

```
se-10-50-10-125> show software versions
```

```
Cisco Unified SIP Proxy version (0.0.11)
Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2008 by Cisco
Systems, Inc.
```

show trace log

To display trace log files on the Cisco Unified SIP Proxy service module, use the **show logs** command in Cisco Unified SIP Proxy EXEC mode.

show trace log

Syntax Description This command has no arguments or keywords.

Command Modes Cisco Unified SIP Proxy EXEC (cusp)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use this command to display the contents of the Cisco Unified SIP Proxy trace log.

Examples In the following example, the **show trace log** command shows the log files on the Cisco Unified SIP Proxy service module.

```
se-Module> show trace log

[DsTransportListener-1] DEBUG 2008.12.22 17:53:39:461 DsSipLlApi.Wire - Received
  UDP packet on 192.168.20.101:6060 ,source 192.168.20.5:6080
INVITE sip:18005551212@192.1.1.75:6061 SIP/2.0
Via: SIP/2.0/UDP 192.168.20.5:6080;branch=z9hG4bK-1-0
From: sipp <sip:sipp@192.168.20.5:6080>;tag=1
To: sut <sip:18005551212@192.1.1.75:6061>
Call-ID: 1-15763@192.168.20.5
CSeq: 1 INVITE
Contact: sip:sipp@192.168.20.5:6080
Max-Forwards: 70
P-Asserted-Identity: <sip:alice@home1.net>
Cisco-Guid: 1234567890
Subject: Performance Test
Content-Type: application/sdp
Content-Length: 135

v=0
o=user1 53655765 2353687637 IN IP4 192.168.20.5
s=-
c=IN IP4 192.168.20.5
t=0 0
m=audio 6070 RTP/AVP 0
a=rtpmap:0 PCMU/8000

--- end of packet ---

[DsTransportListener-1] DEBUG 2008.12.22 17:53:39:492 DsSipLlApi.Wire - Received
  UDP packet on 192.168.20.101:6060 ,source 192.168.20.5:6080
INVITE sip:18005551212@192.1.1.75:6061 SIP/2.0
```

show trace log

```
Via: SIP/2.0/UDP 192.168.20.5:6080;branch=z9hG4bK-2-0
From: sipp <sip:sipp@192.168.20.5:6080>;tag=2
To: sut <sip:18005551212@192.1.1.75:6061>
Call-ID: 2-15763@192.168.20.5
CSeq: 1 INVITE
Contact: sip:sipp@192.168.20.5:6080
Max-Forwards: 70
P-Asserted-Identity: <sip:alice@home1.net>
Cisco-Guid: 1234567890
Subject: Performance Test
Content-Type: application/sdp
Content-Length: 135
```

```
v=0
o=user1 53655765 2353687637 IN IP4 192.168.20.5
s=-
c=IN IP4 192.168.20.5
t=0 0
m=audio 6070 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

```
--- end of packet ---
```

```
[DATAI.0] DEBUG 2008.12.22 17:53:39:508 DsSipLlApi.TransactionManagement - proce
ssMessage(): ----- BEGINING PROCESSING NEW MESSAGE -----
INVITE sip:18005551212@192.1.1.75:6061 SIP/2.0
Via: SIP/2.0/UDP 192.168.20.5:6080;branch=z9hG4bK-1-0
Max-Forwards: 70
```

Related Commands

Command	Description
trace disable	Disables tracing.
trace enable	Enables tracing.
trace level	Sets the trace level.

show startup-config

To display the current startup configuration, use the **show startup-config** command in Cisco Unified SIP Proxy EXEC mode.

show startup-config [paged]

Syntax Description	paged	(Optional) Displays enough output to fill the current viewing screen.
--------------------	--------------	---

Command Modes	Cisco Unified SIP Proxy EXEC
---------------	------------------------------

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced .

Usage Guidelines	This command displays the startup configuration stored in flash memory.
------------------	---

Examples The following is sample output for the **show startup-config** command:

```
se-10-0-0-0> show startup-config

! This adds all the platform CLI commands
!

! hostname
hostname se-10-0-0-0

! Domain Name
ip domain-name localdomain

! DNS Servers
ip name-server 10.100.10.130

! Timezone Settings
clock timezone America/Los_Angeles
end
```

Related Commands	Command	Description
	copy ftp	Copies network FTP server data to another location.
	copy running-config	Copies the running configuration to another location.
	copy startup-config	Copies the startup configuration to another location.
	copy tftp	Copies network TFTP server data to another location.
	erase startup-config	Deletes configuration data.
	show running-config	Displays the running configuration.
	write	Copies the running configuration to the startup configuration.

show version

To display versions of Cisco Unified SIP Proxy components, use the **show version** command in module EXEC mode.

show version

Syntax Description This command has no arguments or keywords.

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use this command to display a list of the installed Cisco Unified SIP Proxy hardware components with their versions and serial numbers.

Examples

```
se-10-0-0-0> show version
se-10-1-1-20> show version
se-10-1-1-20 uptime is 0 weeks, 0 days, 20 hours, 0 minutes
CPU Model:                               Intel(R) Celeron(R) M processor          1.00GHz
CPU Speed (MHz):                         1000.192
CPU Cache (KByte):                       512
BogoMIPS:                               2002.02
SKU:                                     NME-APPRE-522
Chassis Type:                             C2821
Chassis Serial:                           FHK0945F1TA
Module Type:                               NME
Module Serial:                             FOC10480BFM
UDI Name:                                 Not Available
UDI Description:                           Not Available
IDE Drive:                                64MB
SATA Drive:                               80.0GB
SDRAM (MByte):                             512
```

Table 14 describes the significant fields shown in the display.

Table 14 *show version Field Descriptions*

Field	Description
CPU Model	Model of the Cisco Unified SIP Proxy service module CPU.
CPU Speed (MHz)	CPU speed, in megahertz.
CPU Cache (KByte)	Size of the CPU cache, in kilobytes.
Chassis Type	Type of chassis of the Cisco Unified SIP Proxy service module.
Chassis Serial	Serial number of the chassis.

Table 14 *show version Field Descriptions (continued)*

Field	Description
Module Type	A Cisco Network Module (Cisco NME).
Module Serial	Serial number of the Cisco Unified SIP Proxy service module.
SATA Drive	Hard drive on the Cisco Unified SIP Proxy service module.
SKU	Unique ordering identifier for a Cisco Unified SIP Proxy module.

Related Commands

Command	Description
show software	Displays the version numbers of the installed Cisco Unified SIP Proxy software components.

snmp-server community

To set up the community access string to permit access to the Simple Network Management Protocol (SNMP), use the **snmp-server community** command in global configuration mode. To remove the specified community string, use the **no** form of this command.

snmp-server community *string* [**ro** | **rw**]

no snmp-server community *string*

Syntax Description

<i>string</i>	Community string that consists of 1 to 32 alphanumeric characters and functions much like a password, permitting access to SNMP. Blank spaces are not permitted in the community string. Note The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.
ro	(Optional) Specifies read-only access. Authorized management stations can retrieve only MIB objects.
rw	(Optional) Specifies read-write access. Authorized management stations can both retrieve and modify MIB objects.

Command Default

An SNMP community string permits read-only access to all objects.

Command Modes

Global configuration (config)

Command History

Cisco Unified SIP Proxy Version	Modification
8.5.2	This command was introduced.

Usage Guidelines

The **no snmp-server** command disables all versions of SNMP (SNMPv1, SNMPv2C, SNMPv3).

The first **snmp-server** command that you enter enables all versions of SNMP.

To configure SNMP community strings for the MPLS LDP MIB, use the **snmp-server community** command on the host network management station (NMS).



Note

The @ symbol is used as a delimiter between the community string and the context in which it is used. For example, specific VLAN information in BRIDGE-MIB may be polled using community@VLAN_ID (for example, public@100) where 100 is the VLAN number. Avoid using the @ symbol as part of the SNMP community string when configuring this command.

Examples

The following example shows how to set the read/write community string to newstring:

```
Router(config)# snmp-server community newstring rw
```

The following example shows how to remove the community comaccess:

```
Router(config)# no snmp-server community comaccess
```

The following example shows how to disable all versions of SNMP:

```
Router(config)# no snmp-server
```

Related Commands

Command	Description
snmp-server enable	Enables the router to send SNMP notification messages to a designated network management workstation.
snmp-server host	Specifies the targeted recipient of an SNMP notification operation.

snmp-server contact

To set the system contact (sysContact) string, use the **snmp-server contact** command in global configuration mode. To remove the system contact information, use the no form of this command.

snmp-server contact *text*

no snmp-server contact

Syntax Description

<i>text</i>	String that describes the system contact information.
-------------	---

Command Modes

Global configuration (config)

Command History

Cisco Unified SIP Proxy Version	Modification
8.5.2	This command was introduced.

Examples

The following is an example of a system contact string:

```
Router(config)# snmp-server contact Dial System Operator at beeper # 27345
```

Related Commands

Command	Description
snmp-server location	Sets the system location string.

snmp-server enable traps

To enable Simple Network Management Protocol (SNMP) notification types that are available on your system, use the **snmp-server enable traps** command in global configuration mode. To enable a specific trap, follow **snmp-server enable traps** with the command relevant to that trap. To disable all available SNMP notifications, use the no form of this command.

snmp-server enable traps [**All** | **System-State** | **Server-Group** | **SG-Element** | **CPU-Rising** | **CPU-Falling** | **License-State** | **License-Exceeded**]

no snmp-server enable traps

Syntax Description

All	Enable all traps.
System-State	Enable System state trap.
Server-Group	Enable System Group trap.
SG-Element	Enable Server Group Element trap.
CPU-Rising	Enable CPU rising trap.
CPU-Falling	Enable CPU falling trap.
License-State	Enable License state trap.
License-Exceeded	Enable License exceeded trap.

Defaults

No notifications controlled by this command are sent.

Command Modes

Global configuration (config)

Command History

Cisco Unified SIP Proxy Version	Modification
8.5.2	This command was introduced.

Usage Guidelines

Enabling SNMP trap is a two step process. The first step is to activate the command **snmp-server enable traps**, followed by the command specific to the required trap (Commands specific to traps include **All**, **System-State**, **Server-Group**, **SG-Element**, **CPU-Rising**, **CPU-Falling**, **License-State**, and **License-Exceeded**). The second step is to enable the global command **snmp-server enable traps** to enable SNMP functionality on Cisco Unified SIP Proxy Release 9.1. Traps are sent to the host only when this global command is enabled.

For example, you can use **snmp-server enable traps All** to activate all traps, and follow it up with the global command **snmp-server enable traps** to ensure that the trap is generated and sent to the host.

Examples

The following example shows how to enable the router to send all traps to the host specified by the name myhost.cisco.com, using the community string defined as public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com public
```

Related Commands

Command	Description
snmp-server host	Specifies whether you want the SNMP notifications sent as traps, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the destination host (recipient) for the notifications.

snmp-server host

To specify the recipient of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** command in global configuration mode. To remove the specified host from the configuration, use the **no** form of this command.

snmp-server host *ip-address community-string*

no snmp-server host *ip-address community-string*

Syntax Description

<i>ip-address</i>	IPv4 address or IPv6 address of the SNMP notification host.
<i>community-string</i>	Password-like community string sent with the notification operation.
Note	You can set this string using the snmp-server host command by itself, but we recommend that you define the string using the snmp-server community command prior to using the snmp-server host command.
Note	The “at” sign (@) is used for delimiting the context information.

Command Default

This command behavior is disabled by default. A recipient is not specified to receive notifications.

Command Modes

Global configuration (config)

Command History

Cisco Unified SIP Proxy Version	Modification
8.5.2	This command was introduced.

Usage Guidelines

When you enter this command, the default is to send all notification-type traps to the host.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host.



Note

If a community string is not defined using the **snmp-server community** command prior to using this command, the default form of the **snmp-server community** command will automatically be inserted into the configuration. The password (community string) used for this automatic configuration of the **snmp-server community** will be the same as that specified in the **snmp-server host** command. This automatic command insertion and use of passwords is the default behavior for Cisco IOS Release 12.0(3) and later releases.

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely than traps to reach their intended destination.

Compared to traps, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once; an inform may be tried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the router to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no optional keywords, all trap types are enabled for the host.

To enable multiple hosts, you must issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command will be in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command will replace the first.

The **snmp-server host** command is used in conjunction with the **snmp-server enable** command. Use the **snmp-server enable** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

Examples

The following example shows how to enable the router to send all traps to the host 192.30.2.160 using the community string public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host 192.30.2.160 public
```

Related Commands

Command	Description
snmp-server enable traps	Enables SNMP notifications (traps and informs).

snmp-server location

To set the system location string, use the **snmp-server location** command in global configuration mode. To remove the location string, use the **no** form of this command.

snmp-server location *text*

no snmp-server location

Syntax Description

<i>text</i>	String that describes the system location information.
-------------	--

Command Default

No system location string is set.

Command Modes

Global configuration

Command History

Cisco Unified SIP Proxy Version	Modification
8.5.2	This command was introduced.

Examples

The following example shows how to set a system location string:

```
Router(config)# snmp-server location Building 3/Room 214
```

Related Commands

Command	Description
snmp-server contact	Sets the system contact (sysContact) string.

write

To erase, copy, or display the running configuration, use the **write** command in Cisco Unified SIP Proxy EXEC mode.

write [erase | memory | terminal]

Syntax Description

erase	Erases the running configuration.
memory	Writes the running configuration to the startup configuration. This is the default.
terminal	Displays the running configuration.

Defaults

No default behavior or values.

Command Default

None

Command Modes

Cisco Unified SIP Proxy EXEC (cusp)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use the **write** or **write memory** command as a shortcut for the **copy running-config startup-config** command.

Related Commands

Command	Description
erase startup-config	Deletes the current start up configuration.

■ write

■ write

■ write

■ write

■ write

■ write

■ write

■ write

 write

■ write

■ write

■ write

■ write

■ write

■ write

■ write

■ write

■ write

■ write