Cisco Application eXtension Platform 1.1 Command Reference

Last updated: 9/30/08
Text Part Number: OL-15872-02

This guide contains the following sections:

Entering and Exiting the Command Environment

This section describes the procedures for entering and exiting the command environment where Cisco AXP configuration commands are executed, and consists of the following sections:

EXEC and Configuration Modes

The Cisco AXP EXEC and Cisco AXP configuration command modes are similar to the EXEC and configuration modes for Cisco IOS CLI commands.

- Cisco AXP EXEC mode. This mode is similar to Cisco IOS Privileged EXEC mode.

  ```
  se-Module>
  ```

- Cisco AXP application service EXEC mode.

  ```
  se-Module> app-service application-name
  ```

  Example:

  ```
  se-Module> app-service helloworld
  se-Module(exec-helloworld)>
  ```

- Cisco AXP configuration mode.

```
se-Module> configure terminal
se-Module(config)>
```

- Cisco AXP application service configuration mode.

  Example:

```
se-Module(config)> app-service helloworld
se-Module(config-helloworld)>
```

- Cisco AXP syslog application service configuration mode.

  Example:

```
se-Module(config)> app SYSLOG_APP1
se-Module(config-SYSLOG_APP1)>
```

- Cisco AXP interface configuration mode.

  Example:

```
se-Module (config-interface)> ip route table 10
```

Entering the Command Environment

After the Cisco AXP is installed and active, use this procedure to enter the command environment.

Prerequisites

The following information is required to enter the command environment:

- IP address of the ISR router that contains the Cisco AXP service module
- Username and password to log in to the router
- Slot number of the module

SUMMARY STEPS

1. Open a Telnet session.
2. **telnet** *ip-address*
3. Enter the user ID and password of the router.
4. **service-module service-engine** *slot*/*port* **session**
5. **enable** (Optional)

DETAILED STEPS

	Command or Action	Purpose
Step 1	Open a Telnet session.	Use a Microsoft DOS window, a secure shell, or a software emulation tool such as Reflection.
Step 2	**telnet** *ip-address* **Example:** `C:\> telnet 172.16.231.195`	Specifies the IP address of the router.
Step 3	`Username:` `Password:`	Enter your user ID and password for the router.
Step 4	**service-module integrated-service-engine** *slot/port* **session** **Example:** `Router# service-module integrated-service-engine 1/0 session`	Enters the Cisco AXP command environment using the module located in *slot* and *port*. The prompt changes to "se" with the IP address of the service module. If the message "`Trying ip-address slot/port ... Connection refused by remote host`" appears, enter the command: **service-module integrated-service-engine** *slot/port* **session clear** and retry Step 4.
Step 5	**enable** (Optional)	

Exiting the Command Environment

To leave the Cisco AXP command environment and return to the Cisco ISR 2800 command environment, use the **exit** command.

Example:

```
se-Module> exit
Router#
```

Cisco AXP 1.1 Commands

- **app-service (config)**
- **app-service (EXEC)**
- **bind interface**
- **bind serial**
- **clear core**
- **clear cores**
- **clear counters interfaces**
- **clear crashbuffer**
- **clear history**

- clear log
- clear logs
- clear netconf session
- clear syslog-server logs
- clear syslog-server log name
- clock timezone
- connect console
- copy core
- copy ftp
- copy ldap
- copy log
- copy logs bundle
- copy nvram:startup-config
- copy running-config
- copy startup-config
- copy sysdb
- copy syslog-server log name
- copy syslog-server logs bundle
- copy system:running-config
- copy tftp
- copy url
- erase startup-config
- hostname
- interface
- ip access-list standard
- ip address
- ip domain-name
- ip local policy route-map
- ip name-server
- ip route
- ip route table
- ip ssh interface
- ip ssh server
- ip ssh username
- limit cpu utilization
- limit disk utilization
- limit log-file size
- limit memory utilization

- log console
- log console monitor
- log trace boot
- log trace buffer save
- log trace local enable
- log trace server
- log server address
- log level
- netconf
- ntp server
- reload apps
- reset
- route-map
- service password-encryption
- status-monitor
- show app-service state
- show app-service statistics
- show app-service status-monitor
- show arp
- show clock detail
- show configuration
- show cores
- show crash buffer
- show debugging
- show device serial
- show errors
- show history iosapi
- show hosts
- show interfaces
- show ip access-list
- show ip route
- show license udi
- show log name
- show logging
- show logs
- show memory
- show netconf session
- show ntp associations

- show ntp config
- show ntp servers
- show ntp source
- show ntp status
- show packets
- show parser
- show process
- show processes
- show resource limits
- show running-config
- show software
- show ssh-server
- show startup-config
- show state
- show statistics
- show statistics app
- show status-monitor
- show swap usage
- show syslog-server logs
- show syslog-server log name
- show system language
- show tech-support
- show trace buffer
- show trace store
- show trace store-prev
- show version
- software download abort
- software download clean
- software download secure
- software download server
- software download status
- software download upgrade
- software install add
- software install clean
- software install downgrade
- software install upgrade
- software remove
- software uninstall

- syslog-server
- syslog-server limit file-rotation
- syslog-server limit file-size
- system language preferred
- techsupport support shell
- trace
- username ios
- username sysadmin
- write

app-service (config)

To configure the Cisco AXP application hosting environment for a specific application, use the **app-service** command in Cisco AXP configuration mode.

app-service *app-name*

Syntax Description

app-name	Application name

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP Configuration Mode.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, the configuration mode for application "helloworld" is entered.

```
se-Module(config)> app-service helloworld
se-Module(config-helloworld)>
se-Module(config-helloworld)> ?
  <cr>
  bind         Device Binding
  exit         Leave app-service configuration mode
  hostname     Set the system name
  ip           IP configuration
  limit        Limit resource usage
  log          System event messages
  shutdown     stop or start the hosting environment
  status-monitor Application Status Monitor
```

Related Commands

Command	Description
show state	Displays the state and health of the specified application.

app-service (EXEC)

To configure the Cisco AXP application hosting environment for a specific application, use the **app-service** command in Cisco AXP EXEC mode.

app-service *app-name*

Syntax Description

app-name	Application name

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC Mode.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, the EXEC mode for application “helloworld” is entered.

```
se-Module(exec-helloworld)> ?
  <cr>
  clear        Reset functions
  connect      Cross connect to hosting environment
  copy         Copy data from one location to another
  end          Leave app-service exec mode
  reset        Reset the hosting environment
  show         Show running system information
```

Related Commands

Command	Description
show state	Displays the state and health of the specified application.

bind interface

To attach a networking device to the application environment, use the **bind interface** command in Cisco AXP application service configuration mode. To detach a networking device from the application environment, use the **no** form of this command.

bind interface *network-interface-name*

no bind interface *network-interface-name*

Syntax Description

network-interface-name	Interface name defined in the host.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP application service configuration.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

This command attaches or detaches a networking device to or from the application environment. The *network-interface-name* is the interface name defined in the host, for example, the Ethernet *device-name* defined in the **interface** command.

The interface is immediately available to the virtual instance with the execution of a new **bind** command.

Removing an interface binding with the **no** prefix displays the following warning messages:

```
WARNING!!! Reset the hosting environment

WARNING!!! For binding to be removed
```

Note This command modifies configuration entries in the */etc/hosts* file for *ipaddr* and *hostname* mapping.

ipaddr in the /etc/hosts file is modified when you enter the **bind interface** command (eth0 is the default).

Examples

In the following example, the Cisco AXP application service EXEC mode for application “helloworld” is entered, then the **bind** command attaches pre-defined interface eth0 to the application.

```
se-Module(config)> app-service helloworld
se-Module (config-helloworld)> bind interface eth0
```

Related Commands

Command	Description
interface	Configures the network interfaces.

bind serial

To attach or bind the serial device to the application environment, use the **bind serial** command in Cisco AXP application service configuration mode. To unattach the serial device to the application environment, use the **no** form of the command.

bind serial *device-id* [*device-id on hosting environment*]

no bind serial *device-id* [*device-id on hosting environment*]

Syntax Description

device-id	Device ID of the serial device connected to the IOS side.
device-id on hosting environment	(Optional) Device name in hosting environment, which is different from the device ID (*device-id*) on the Cisco IOS side.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP application service configuration.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

This command typically follows the **app-service** <application name> command.The application being a serial application.

Examples

In the following example, the Cisco AXP application service configuration mode for the serial device “serialapp” is entered. Then the serial device is bound to a Cisco IOS side device id of “vtty000”.

```
se-Module(config)> app-service serialapp
se-Module(config-serialapp)> bind serial vtty000 modem
```

Related Commands

Command	Description
app-service	Enters Cisco AXP application hosting environment for a specific application.
show device serial	Displays the device ID.

clear core

To clear one specific core file of an application, use the **clear core** command in Cisco AXP application service EXEC mode.

clear core name *core-name*

Syntax Description

core-name	Name of the core file.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP application service EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, the helloworld-test-core-file is cleared from the application:

```
se-Module(exec-helloworld)> clear core name helloworld-test-core-file
```

Related Commands

Command	Description
show cores	Displays all core files.

clear cores

To clear all of an application's core files, use the **clear cores** command in Cisco AXP application service EXEC mode.

clear cores

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP application service EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, clear the core files of a Cisco AXP application in Cisco AXP application service EXEC mode:

```
se-Module(exec-helloworld)> clear cores
```

Related Commands

Command	Description
show cores	Displays all core files.

clear counters interfaces

To clear the statistical counters, use the **clear counters interfaces** command in Cisco AXP EXEC mode.

clear counters interfaces {**gigabitEthernet** *unit-number* | **ide 0**}

Syntax Description

gigabitEthernet	Interface counter of GigabitEthernet IEEE 802.3 interface unit number.
unit-number	GigabitEthernet unit number 0 or 1.
ide	Interface counter of Integrated Drive Electronics hard disk drive.
0	Disk unit number of local hard disk drive.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, the interface counter of the GigabitEthernet unit number 0 is cleared:

```
se-Module> clear counters interfaces gigabitethernet 0
se-Module>
```

Related Commands

Command	Description
show interfaces	Displaces the interfaces and related statistics.

clear crashbuffer

To clear the kernel crash buffer, use the **clear crashbuffer** command in Cisco AXP EXEC mode.

clear crashbuffer

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, the kernel crash buffer is cleared:

```
se-Module> clear crashbuffer
se-Module>
```

Related Commands

Command	Description
show crash buffer	Displays the kernel crash buffer contents.

clear history

To clear the command-line interface (CLI) history records, use the **clear history** command in Cisco AXP EXEC mode.

clear history *app-service* [*record-number*] | **config** [*record-number*] | **exec** [*record-number*]}

Syntax Description

app-service	Clears the application service CLI history records.
record-number	(Optional) Clears the number of application service CLI history records in the range of 1 to 100.
config	Clears configuration mode application service CLI.
record-number	(Optional) Clears the number of configuration mode application service CLI history records in the range of 1 to 70.
exec	Clears executive mode application service CLI.
record-number	(Optional) Clears the number of executive mode application service CLI history records in the range of 1 to 30.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, the 10th CLI history record of the IOSAPI application service are cleared:

```
se-Module> clear history iosapi 10
se-Module>
```

Related Commands

Command	Description
show history	Displays application service CLI history.

clear log

In Cisco AXP application service EXEC mode, use the **clear log** command to clear the content of a specific log file of the application.

In Cisco AXP EXEC mode, use the **clear log** command to clear the content of a specific host log file.

clear log name *log-name*

Syntax Description

log-name	Name of the specific log file.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP application service EXEC.

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

Depending on the mode, use this command to either clear the contents of a specific host log file (Cisco AXP EXEC mode) or clear the contents of a specific application log file (Cisco AXP application service EXEC mode).

Note In Cisco AXP EXEC mode, the command does not clear a syslog server log file.

Examples

In the following example, the log file messages.log is cleared in Cisco AXP application service EXEC mode:

```
se-Module(exec-helloworld)> clear log name messages.log
```

In the following example, the log file sshd.log is cleared in Cisco AXP EXEC mode:

```
se-Module> clear log name sshd.log
```

Related Commands

Command	Description
show logs	Displays all log files.

clear logs

In Cisco AXP application service EXEC mode, use the **clear logs** command to clear the content of all log files of the application.

In Cisco AXP EXEC mode, use the **clear logs** command to clear the content of all host log files.

clear logs

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP application service EXEC.

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

Depending on the mode, the command either clears the contents of all host log files (Cisco AXP EXEC mode) or clears the contents of the application log files (Cisco AXP application service EXEC mode).

Note In Cisco AXP EXEC mode, the command does not clear syslog server log files.

Examples

In the following example, the log files are cleared in Cisco AXP application service EXEC mode:

```
se-Module(exec-helloworld)> clear logs
```

In the following example, the log files are cleared in Cisco AXP EXEC mode:

```
se-Module> clear logs
```

Related Commands

Command	Description
show logs	Displays a list of logs.

clear netconf session

To clear the network configuration management system session identifier, use the **clear netconf session** command in Cisco AXP EXEC mode.

clear netconf session *session-id* [|]

Syntax Description

session-id	Network configuration management system session identifier.
|	(Optional) Pipes output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, the kernel crash buffer is cleared:

```
se-Module> clear netconf session 23
se-Module>
```

Related Commands

Command	Description
show netconf	Displays the network configuration management system information.

clear syslog-server logs

To clear the content of all syslog files in the /var/remote directory, use the **clear syslog-server logs** command in Cisco AXP EXEC mode.

clear syslog-server logs

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, the content of all syslog files in the /var/remote directory is cleared:

```
se-Module> clear syslog-server logs
```

Related Commands

Command	Description
show syslog-server logs	Displays a list of syslog server log files.

clear syslog-server log name

To clear the contents of a specific syslog server file, use the **clear syslog-server log-name** command in Cisco AXP EXEC mode.

clear syslog-server log name *log-name*

Syntax Description

log-name	Name of the specific syslog server log file.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, the contents of a specific syslog server file are cleared:

```
se-Module> clear syslog-server log name remote_messages.log
```

Related Commands

Command	Description
show syslog-server log	Displays recent syslog server log messages.

clock timezone

To set the time zone for the Cisco AXP service module, use the **clock timezone** command in Cisco AXP configuration mode.

To remove the time zone configuration, use the **no** form of this command .

clock timezone [*time-zone*]

no clock timezone [*time-zone*]

Syntax Description

time-zone	(Optional) Time zone of the local branch.

Command Modes

Cisco AXP configuration.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

The configured NTP server provides the date-stamp system and application functions. The **clock timezone** command specifies the local time zone where Cisco AXP is installed.

If you know the phrase for the time-zone, enter it for the *time-zone* value. For example, to directly configure the time zone for UTC in Cisco AXP 1.1, use the **clock timezone UTC** command. For Cisco AXP releases prior to 1.1, use **clock timezone Etc/UTC**.

If you do not know the time zone phrase, leave the *time-zone* value blank and a series of menus appear to guide you through the time zone selection process. Press ctrl-c any time to exit this menu.

Bash Shell

To select the time zone in the Bash shell, use the **tzselect** command and click <Enter> for a series of menus to guide you through your selection.

Examples

In the following example, the United States Pacific Time is selected from the timezone menu:

```
se-10-0-0-0> config t
Enter configuration commands, one per line.  End with CNTL/Z.
se-10-0-0-0(config)> clock timezone

Press ctrl-c at any time to exit this menu

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                 27) Honduras
2) Antigua & Barbuda        28) Jamaica
```

```
3) Argentina                29) Martinique
4) Aruba                    30) Mexico
5) Bahamas                  31) Montserrat
6) Barbados                 32) Netherlands Antilles
7) Belize                   33) Nicaragua
8) Bolivia                  34) Panama
9) Brazil                   35) Paraguay
10) Canada                   36) Peru
11) Cayman Islands           37) Puerto Rico
12) Chile                    38) St Barthelemy
13) Colombia                 39) St Kitts & Nevis
14) Costa Rica               40) St Lucia
15) Cuba                     41) St Martin (French part)
16) Dominica                 42) St Pierre & Miquelon
17) Dominican Republic       43) St Vincent
18) Ecuador                  44) Suriname
19) El Salvador              45) Trinidad & Tobago
20) French Guiana            46) Turks & Caicos Is
21) Greenland                47) United States
22) Grenada                  48) Uruguay
23) Guadeloupe               49) Venezuela
24) Guatemala                50) Virgin Islands (UK)
25) Guyana                   51) Virgin Islands (US)
26) Haiti
#? 47
Please select one of the following time zone regions.
1) Eastern Time
2) Eastern Time - Michigan - most locations
3) Eastern Time - Kentucky - Louisville area
4) Eastern Time - Kentucky - Wayne County
5) Eastern Time - Indiana - most locations
6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
7) Eastern Time - Indiana - Starke County
8) Eastern Time - Indiana - Pulaski County
9) Eastern Time - Indiana - Crawford County
10) Eastern Time - Indiana - Switzerland County
11) Central Time
12) Central Time - Indiana - Perry County
13) Central Time - Indiana - Pike County
14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
15) Central Time - North Dakota - Oliver County
16) Central Time - North Dakota - Morton County (except Mandan area)
17) Mountain Time
18) Mountain Time - south Idaho & east Oregon
19) Mountain Time - Navajo
20) Mountain Standard Time - Arizona
21) Pacific Time
22) Alaska Time
23) Alaska Time - Alaska panhandle
24) Alaska Time - Alaska panhandle neck
25) Alaska Time - west Alaska
26) Aleutian Islands
27) Hawaii
#? 21

The following information has been given:

United States
Pacific Time

Therefore TZ='America/Los_Angeles' will be used.
Is the above information OK?
1) Yes
2) No
```

```
#? 1
se-Module(config)>
```

To select United States Pacific Time using the timezone name:

```
se-Module> config t
se-Module(config)> clock timezone Americas/Los_Angeles
```

Related Commands

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

connect console

To allow third-party applications to integrate their commands to the console shell, use the **connect console** command in Cisco AXP application service EXEC mode.

connect console

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP application service EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

This command allows a third party to integrate their own application commands to the console shell. On initiating the command, /bin/console is executed. The third party application must provide its own console file in binary or a script (telnet to their CLI), to cross connect to its CLI shell.

If the application does not provide a console file, the following message appears:

```
Unable to start console
```

Examples

In the following example, the shell of an application's virtual instance is entered:

```
se-Module(exec-tcptrace)> connect console <enter>
bash-2.05b#
```

Related Commands

Command	Description
show tech-support	Displays system details.

copy core

To copy a core file to another location, use the **copy core** command in Cisco AXP EXEC mode.

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

Syntax Description

core-name	Filename used to identify the core.
url	Destination Universal Resource Location (URL).
ftp/http url	FTP or HTTP URL destination location to which the core file is to be copied.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

When you copy a core file, the **copy core** command becomes interactive and prompts you for the necessary file destination URL information. Use the **show core** command to view the core.

The standard FTP URL format is supported:

ftp://[user-id:ftp-password@]ftp-server-address[/directory]

Examples

In the following example, the file mping-test-file2 is copied to remote URL http://example.net.

```
se-Module(exec-helloworld)> copy core mping-test-file2 http://example.net
```

Related Commands

Command	Description
show cores	Displays the list of core files.

copy ftp

To copy a new configuration from an FTP server to another location, use the **copy ftp** command in Cisco AXP 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

Cisco AXP EXEC

Command History

Cisco AXP Version	Modification
1.1	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.

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

Related Commands

Command	Description
show running-config	Displays the content of the current running configuration.
show startup-config	Displays the content of the startup configuration.

copy ldap

To copy the current LDAP information stored in the local database to an FTP server, use the **copy ldap** command in Cisco AXP EXEC mode.

copy ldap url ftps://[*user-id:ftp-password@*]*ftp-server-address*[*/directory*]*/filename*

Syntax Description

url ftps://*user-id***:***ftp-password***@**	(Optional) Specifies the FTP username and password to access the FTP server. If no username and password are specified, the default username anonymous is used.
@ftp-server-address	The IP address of the FTP server.
/directory	(Optional) The directory where the LDAP data file will be stored on the FTP server. If no directory is specified, the default directory on the FTP server will be used.
/filename	The filename for the LDAP data on the FTP server.

Command Modes

Cisco AXP EXEC

Command History

Cisco Unity Express Release	Modification
1.1	This command was introduced .

Usage Guidelines

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

Examples

The following example shows copying the LDAP data to the default directory on the FTP server and saving the data in the file ldapinfo.

```
se-Module# copy ldap url ftps://admin:cue@10.10.67.163/ldapinfo
se-Module#
```

Related Commands

Command	Description
show sysdb	Displays content of the system configuration database.

copy log

To copy an application log file to a remote URL, use the **copy log** command in Cisco AXP application service EXEC mode.

To copy a Cisco AXP host operating system log file to a remote URL, use the **copy log** command in Cisco AXP EXEC mode.

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

Syntax Description

log-name	Log filename
ftp/http url	FTP/HTTP address

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP application service EXEC.

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command, in Cisco AXP application service EXEC mode, to copy syslog, trace and custom application log files for a specific application to a remote URL. The standard ftp URL format is supported:

ftp://[user-id:ftp-password@]ftp-server-address[/directory]

The log filename (in both command modes) may contain wildcards * allowing the copying of more than one log file at a time.

Examples

In the following example, the **copy log** command copies log file install.log from application “mping” to a remote server:

```
se-Module(exec-mping)> copy log install.log url ftp://admin:mpg@10.10.67.163/lnstallinfo
```

Related Commands

Command	Description
show log	Displays recent system event messages.

copy logs bundle

To copy a tar file containing syslog files and custom application log files on the guest operating system to a remote URL, use the **copy logs bundle** command in Cisco AXP application service EXEC mode.

To copy a tar file containing syslog files and custom application log files on the guest and host operating systems to a remote URL, use the **copy logs bundle** command in Cisco AXP EXEC mode.

copy logs bundle *destfilename***.tar url** *url*

Syntax Description

destfilename	Tar filename
url	Destination URL.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP application service EXEC.

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

If you are in In Cisco AXP EXEC mode, this command does not copy remote syslog server log files.

Examples

In the following example, a tar file is copied to a remote server:

```
se-Module(exec-mping)> copy logs bundle mpg.tar url http://lab:mpg@10.10.67.163/appinfo
```

Related Commands

Command	Description
show logs	Displays a list of log messages.

copy nvram:startup-config

To copy the NVRAM startup configuration to another destination, use the **copy nvram:startup-config** command in Cisco AXP EXEC mode.

copy nvram:startup-config {**ftp: | tftp: | url** *ftps/https-url* **username** *username* **password** *password*}

Syntax Description

ftp:	Begins the FTP menu where you enter the FTP server IP address and destination filename to copy the startup configuration to an FTP server.
tftp:	Begins the TFTP menu where you enter the TFTP server IP address and destination filename to copy the startup configuration to a TFTP server.
url	Destination Universal Resource Location (URL).
ftps/https-url	FTPS or HTTPS secure URL destination location to which the running-config file is to be copied. Enter your username and password for a secure connection.
username *username* **password** *password*	Enter username and password to access secure server.

Command Modes

Cisco AXP EXEC

Command History

Cisco Unity Express Release	Modification
1.1	This command was introduced.

Usage Guidelines

When you copy to an FTP or TFTP server, the **copy nvram:startup-config** 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.

When you copy to an FTPS or HTTPS secure URL destination location, enter your username and password for a secure connection.

Examples

In the following example, the NVRAM startup configuration is copied to the FTP server, which requires a user ID and password and has an IP address of 172.16.231.193. The NVRAM startup configuration is copied to the configs directory as file *saved_start*.

```
se-Module# copy nvram:startup-config ftp:
Address or name of remote host? admin:voice@172.16.231.193/configs
Source filename? saved_start
```

The following example shows the NVRAM startup configuration being copied to the TFTP server as filename *temp_start*:

```
se-Module# copy nvram:startup-config tftp:
Address or name of remote host? 172.16.231.190
Source filename? temp_start
```

The following example shows the NVRAM startup configuration being copied to a secure URL, where the server hostname is *lyons*, the directory is *tigers*, and the filename is *bears*:

```
se-Module# copy nvram:startup-config url ftps://lyons/tigers/bears username wizard
password oz
```

Related Commands

Command	Description
show running-config	Displays the content of the current running configuration.
show startup-config	Displays the content of the startup configuration.

copy running-config

To copy the current running configuration to another destination, use the **copy running-config** command in Cisco AXP EXEC mode.

copy running-config {**ftp: | nvram:startup-config** *filename* **| startup-config | tftp: | url** *ftps/https-url* **username** *username* **password** *password*}

Syntax Description

ftp:	Begins the FTP interactive menu where you enter the FTP server IP address and destination filename to copy the running configuration to an FTP server.
nvram:startup-config *filename*	Copies the running configuration to the NVRAM saved configuration named *filename*.
startup-config	Copies the running configuration to the startup configuration in flash memory named *filename*.
tftp:	Begins the TFTP menu where you enter the TFTP server IP address and destination filename to copy the running configuration to a TFTP server.
url	Destination Universal Resource Location (URL).
ftps/https-url	FTPS or HTTPS secure URL destination location to which the running-config file is to be copied. Enter your username and password for a secure connection.
username *username* **password** *password*	Enter username and password to access secure server.

Command Modes

Cisco AXP EXEC

Command History

Cisco Unity Express Release	Modification
1.1	This command was introduced.

Usage Guidelines

When you copy to an FTP or TFTP server, the **copy running-config** command becomes interactive and prompts you for the necessary information. 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

In the following example, the running configuration is copied to the FTP server, which requires a user ID and password and has an IP address of 172.16.231.193. The running configuration is copied to the configs directory as file saved_start.

```
se-Module# copy running-config ftp:
Address or name of remote host? admin:voice@172.16.231.193/configs
Source filename? saved_start
```

The following example shows the running configuration copied to the NVRAM saved configuration as filename *startup*:

```
se-Module# copy running-config nvram:startup-config startup
```

The following example shows the running configuration copied to the startup configuration as filename *start*:

```
se-Module# copy running-config startup-config start
```

The following example shows the running configuration copied to the TFTP server as filename *temp_start*:

```
se-Module# copy running-config tftp:
Address or name of remote host? 172.16.231.190
Source filename? temp_start
```

The following example shows the running configuration being copied to a secure URL, where the server hostname is *lyons*, the directory is *tigers*, and the filename is *bears*:

```
se-Module# copy running-config url ftps://lyons/tigers/bears username wizard password oz
```

Related Commands

Command	Description
show running-config	Displays the content of the current running configuration.
show startup-config	Displays the content of the startup configuration.

copy startup-config

To copy the startup configuration to another destination, use the **copy startup-config** command in Cisco AXP EXEC mode.

copy startup-config {**ftp:** | **tftp:** | **url** *ftps/https-url* **username** *username* **password** *password*}

Syntax Description

ftp:	Begins the FTP menu where you enter the FTP server IP address and destination filename to copy the startup configuration to an FTP server.
tftp:	Begins the TFTP menu where you enter the TFTP server IP address and destination filename to copy the startup configuration to a TFTP server.
url	Destination Universal Resource Location (URL).
ftps/https-url	FTPS or HTTPS secure URL destination location to which the startup-config file is to be copied. Enter your username and password for a secure connection.
username *username* **password** *password*	Enter username and password to access secure server.

Command Modes

Cisco AXP EXEC

Command History

Cisco Unity Express Release	Modification
1.1	This command was introduced.

Usage Guidelines

When you copy to an FTP or TFTP server, the **copy startup-config** 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.

When you copy to an FTPS or HTTPS secure URL destination location, enter your username and password for a secure connection.

Examples

In the following example, the startup configuration is copied to the FTP server, which requires a user ID and password and has an IP address of 172.16.231.193. The startup configuration is copied to the configs directory as file *saved_start*.

```
se-Module# copy startup-config ftp:
Address or name of remote host? admin:voice@172.16.231.193/configs
Source filename? saved_start
```

The following example shows the startup configuration being copied to the TFTP server as filename *temp_start*:

```
se-Module# copy startup-config tftp:
Address or name of remote host? 172.16.231.190
Source filename? temp_start
```

The following example shows the startup configuration being copied to a secure URL, where the server hostname is *lyons*, the directory is *tigers*, and the filename is *bears*:

```
se-Module# copy startup-config url ftps://lyons/tigers/bears username wizard password oz
```

Related Commands

Command	Description
show startup-config	Displays the content of the startup configuration.

copy sysdb

To copy the system database to another destination, use the **copy sysdb** command in Cisco AXP EXEC mode.

copy sysdb url *ftps/https-url* **username** *username* **password** *password*

Syntax Description

url	Destination Universal Resource Location (URL).
ftps/https-url	FTPS or HTTPS secure URL destination location to which the system database is to be copied. Enter your username and password for a secure connection.
username *username* **password** *password*	Enter username and password to access secure server.

Command Modes

Cisco AXP EXEC

Command History

Cisco Unity Express Release	Modification
1.1	This command was introduced.

Usage Guidelines

When you copy to an FTPS or HTTPS secure URL destination location, enter your username and password for a secure connection.

Examples

The following example shows the startup configuration being copied to a secure URL, where the server hostname is *lyons*, the directory is *tigers*, and the filename is *bears*:

```
se-Module# copy startup-config url ftps://lyons/tigers/bears username wizard password oz
```

Related Commands

Command	Description
show running-config	Displays the content of the current running configuration.
show startup-config	Displays the content of the startup configuration.

copy syslog-server log name

To copy a specific syslog server log file, use the **copy syslog-server log name** command in Cisco AXP EXEC mode.

copy syslog-server log name *log-name* **url** *ftp/http-url*

Syntax Description

log-name	Syslog server log filename.
url	Destination Universal Resource Location (URL).
ftp/http-url	FTP or HTTP URL destination location to which the log file is to be copied.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

The standard FTP URL format is supported:

ftp://[user-id:ftp-password@]ftp-server-address[/directory]

A wildcard * may be used to copy more than one log file at a time.

Related Commands

Command	Description
show syslog-server log	Displays recent syslog server log messages.

copy syslog-server logs bundle

To bundle all the syslog server log files into a gzip file and copy them to a remote URL, use the **copy syslog-server logs bundle** command in Cisco AXP EXEC mode.

copy syslog-server logs bundle *destination-filename***.gz url** *ftp/http-url*

Syntax Description

destination-filename	gzip filename
url	Destination Universal Resource Location (URL).
ftp/http-url	FTP or HTTP URL destination location to which the log file is to be copied.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, the syslog server log files are bundled into a gzip file and copied to a remote URL:

```
se-Module> copy syslog-server logs bundle myappslogs.gz url http://testfiles.company.com
```

Related Commands

Command	Description
show syslog-server logs	Displays the list of log files.

copy system:running-config

To copy the current system running configuration to another destination, use the **copy system:running-config** command in Cisco AXP EXEC mode.

copy system:running-config {**ftp:** | **nvram:startup-config** *filename* | **startup-config** | **tftp:** | **url** *ftps/https-url* **username** *username* **password** *password*}

Syntax Description

ftp:	Begins the FTP interactive menu where you enter the FTP server IP address and destination filename to copy the running configuration to an FTP server.
nvram:startup-config *filename*	Copies the running configuration to the NVRAM saved configuration named *filename*.
startup-config	Copies the running configuration to the startup configuration in flash memory named *filename*.
tftp:	Begins the TFTP menu where you enter the TFTP server IP address and destination filename to copy the running configuration to a TFTP server.
url	Destination Universal Resource Location (URL).
ftps/https-url	FTPS or HTTPS secure URL destination location to which the current system running-config file is to be copied. Enter your username and password for a secure connection.
username *username* **password** *password*	Enter username and password to access secure server.

Command Modes

Cisco AXP EXEC

Command History

Cisco Unity Express Release	Modification
1.1	This command was introduced.

Usage Guidelines

When you copy to an FTP or TFTP server, the **copy system:running-config** command becomes interactive and prompts you for the necessary information. 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

In the following example, the system running configuration is copied to the FTP server, which requires a user ID and password and has an IP address of 172.16.231.193. The system running configuration is copied to the configs directory as file saved_start.

```
se-Module# copy system:running-config ftp:
Address or name of remote host? admin:voice@172.16.231.193/configs
Source filename? saved_start
```

The following example shows the system running configuration copied to the NVRAM saved configuration as filename *startup*:

```
se-Module# copy system:running-config nvram:startup-config startup
```

The following example shows the system running configuration copied to the startup configuration as filename *start*:

```
se-Module# copy system:running-config startup-config start
```

The following example shows the system running configuration copied to the TFTP server as filename *temp_start*:

```
se-Module# copy system:running-config tftp:
Address or name of remote host? 172.16.231.190
Source filename? temp_start
```

The following example shows the system running configuration being copied to a secure URL, where the server hostname is *lyons*, the directory is *tigers*, and the filename is *bears*:

```
se-Module# copy system:running-config url ftps://lyons/tigers/bears username wizard
password oz
```

Related Commands

Command	Description
show running-config	Displays the content of the current running configuration.
show startup-config	Displays the content of the startup configuration.

copy tftp

To copy the network TFTP server information to another destination, use the **copy tftp** command in Cisco AXP EXEC mode.

copy tftp: {**nvram:startup-config** | **running-config** | **startup-config** | **system:running-config**}

Syntax Description

nvram:startup-config	Destination location for the copy procedure is the NVRAM saved configuration. Begins the interactive menu where you enter the TFTP server IP address and destination filename.
running-config	Destination location for the copy procedure is the active configuration in flash memory. Begins the interactive menu where you enter the TFTP server IP address and destination filename.
startup-config	Destination location for the copy procedure is the startup configuration in flash memory. Begins the interactive menu where you enter the TFTP server IP address and destination filename.
system:running-config	Destination location for the copy procedure is the system configuration. Begins the interactive menu where you enter the TFTP server IP address and destination filename.

Command Modes

Cisco AXP EXEC

Command History

Cisco Unity Express Release	Modification
1.1	This command was introduced.

Usage Guidelines

The **copy tftp** command is an interactive command and prompts you for the necessary information. Add a username and password to the server IP address if your server is not configured to accept anonymous TFTP input. The format would be: *userid***:***password@ftp-server-address/directory*. If you do not specify a *directory* value, the software uses the default TFTP directory.

Copying a startup configuration from the TFTP server to the startup configuration overwrites the startup configuration. A warning appears, asking you to confirm the overwrite.

Examples

The following example shows a TFTP server with the IP address 10.3.61.16. The TFTP server data in the source filename start is copied to the running configuration.

```
se-Module# copy tftp: running-config
Address or name of remote host? 10.3.61.16
Source filename? start
```

In the following example, the TFTP server has the IP address 10.3.61.16. The file start in directory configs on the TFTP server is copied to the startup configuration.

```
se-Module# copy tftp: startup-config
!!!WARNING!!! This operation will overwrite your startup configuration.
Do you wish to continue[y]? y
Address or name of remote host? 10.3.61.16/configs
```

```
Source filename? start
```

Related Commands

Command	Description
show running-config	Displays the content of the current running configuration.
show startup-config	Displays the content of the startup configuration.

copy url

To copy the network configuration information to a secure URL, use the **copy url** command in Cisco AXP EXEC mode.

copy url *ftps/https-url* {**nvram:startup-config | running-config | startup-config | system:running-config**} **username** *username* **password** *password*

Syntax Description

url	Destination Universal Resource Location (URL).
ftps/https-url	FTPS or HTTPS secure URL destination location to which the current system running-config file is to be copied. Enter your username and password for a secure connection.
nvram:startup-config	Destination location for the copy procedure is the NVRAM saved configuration.
running-config	Destination location for the copy procedure is the active configuration in flash memory.
startup-config	Destination location for the copy procedure is the startup configuration in flash memory.
system:running-config	Destination location for the copy procedure is the system configuration.
username *username* **password** *password*	Enter username and password to access secure server.

Command Modes

Cisco AXP EXEC

Command History

Cisco Unity Express Release	Modification
1.1	This command was introduced.

Usage Guidelines

The **copy url** command is an interactive command and prompts you for the necessary information. Add a username and password to the server IP address if your server is not configured to accept anonymous TFTP input. The format would be: *userid***:***password@ftp-server-address/directory*. If you do not specify a *directory* value, the software uses the default directory.

Examples

The following example shows the system running configuration being copied to a secure URL, where the server hostname is *lyons*, the directory is *tigers*, and the filename is *bears*:

```
se-Module# copy url ftps://lyons/tigers/bears system:running-config username wizard
password oz
```

Related Commands

Command	Description
show running-config	Displays the content of the current running configuration.
show startup-config	Displays the content of the startup configuration.

erase startup-config

To erase the startup configuration in memory, use the **erase startup-config** command in Cisco AXP EXEC mode.

erase startup-config

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

Before using this command, make sure that your startup configuration has been backed up.

Related Commands

Command	Description
show running-config	Displays the content of the current running configuration.
show startup-config	Displays the content of the startup configuration.

hostname

To configure a hostname for the application that is different from the name used for the host, use the **hostname** command in Cisco AXP 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

name	Hostname for the application.

Defaults

Hostname configured on the host side.

Command Default

None.

Command Modes

Cisco AXP application service configuration.

Command History

Cisco AXP 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 AXP host. The hostname is limited to 32 characters.

If more than 32 characters are entered, the following error message appears:

```
hostname size greater than 32
```

This command modifies configuration directives in file */etc/hosts*. The command updates the hostname of the hostname: IP mapping entry.

If the file does not exist, the command creates the */etc/hosts* file, and adds an entry to the file.

If the file exists, (for example, if an application package has already bundled its own */etc/hosts* file), the new entries are appended to the existing entries and the original entries remain intact.

Examples

In the following example, the initial contents of file etc/hosts are:

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

For example, the following commands set the hostname to “myhostname”. The original hostname is the hostname of the host (after installing the application, the hostname for the vserver is the same as for the host.)

```
configure terminal
app-service myapp
hostname myhostname
```

The hostname in the second line of the /etc/hosts file above, (`ipaddr hostname.domain hostname)` is changed to myhostname.

The /etc/hosts file is created by Cisco AXP if it is not packaged by the user. An /etc/hosts file that is created by the user must contain the first line shown above (starting with "127.0.0.1"). Lines following the first line of the file are created by Cisco AXP.

The IP address, `ipaddr` in the `/etc/hosts` file is modified using the **bind interface** command.

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

Related Commands

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

interface

To configure external network interfaces and enter interface configuration mode, use the **interface** command in Cisco AXP interface configuration mode.

To disable the AXP module interface configuration, use the **no** form of this command.

interface {**eth0** | **eth1**} [**exit** | **ip** {**address** *ip-address ip-mask* | **route table** *table-num*} | **shutdown**]

no interface {**eth0** | **eth1**}

Syntax Description

eth0	Ethernet interface 0.
eth1	Ethernet interface 1.
exit	Leave Cisco AXP interface configuration mode.
ip *ip-address network-mask*	Configure IP interface IP address and network mask.
route table *table-num*	Route table number in the range of 1 to 252.
shutdown	Enables or disables the interface. To disable the interface, use the **no** form of the command: **no shutdown**. **Note** Disabling the physical interface disables associated virtual or VLAN interfaces.

Defaults

None.

Command Default

None.

Command Modes

Cisco AXP interface configuration.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

The device name can be **eth0** or **eth1** for a built-in physical interface, **eth0:1** for a virtual interface, or **eth0.1** for a VLAN interface.

The virtual or VLAN interfaces can be configured only if these interfaces are not bound to the virtual hosting environment. If the interfaces are bound, an error message with the specific device name appears. For example, for **eth0.1**, the following error message appears:

Error Message `eth0.1 still bound to hosting environment(s), unbind first.`

Do not remove a built-in physical interface. On removal, an error message appears:

Error Message `Can not remove the built-in interface eth0/1.`

Examples

In the following example, the command interface eth0 configures the exte**rnal network interface eth0,** by entering interface configuration mode.

```
se-Module (config)> interface eth0
se-Module(config-interface)> ip 10.0.0.0 255.255.255.0
se-Module(config-interface)> route table 126
```

Related Commands

Command	Description
show interfaces	Displays all the interfaces of the Cisco AXP module.
bind interface	Attaches or detaches a networking device to or from the application environment.

ip access-list standard

To configure a predefined, standard access list (ACL) for the application, use the **ip access-list standard** command in Cisco AXP configuration mode.

To remove the IP ACL, use the **no** form of this command.

ip access-list standard *{acl-name | acl-num}*

no ip access-list standard

Syntax Description

acl-name	Name identifier for an access list to which all commands entered in access list configuration mode apply. Format: 30 alphanumeric characters, beginning with a letter.
acl-num	Numeric identifier for an access list to which all commands entered in access list configuration mode apply. Format (for standard access lists): number in the range 1–99.

Defaults

None.

Command Default

None.

Command Modes

Cisco AXP configuration.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to create an access list for source-based route configurations.

To create an entry that specifies the type of packets that you want for further processing, use the **permit** command in standard ACL subcommand mode (config-std-nacl) to specify the type of packets that must be accepted for further processing.

Include at least one permit entry to create a valid access list.

Cisco AXP 1.0 allows only a single IP address in the access list to be specified.

Examples

In the following example, an access list is created for source-based route configuration.

```
se-Module (config)> ip access-list standard test
```

Related Commands

Command	Description
permit	Adds a line to a standard access list specifying the type of packets to be accepted for further processing.
show ip access-list	Displays predefined standard ACLs or ACLs by name.

ip address

To configure the IP address for a network interface, use the **ip address** command in Cisco AXP interface configuration mode.

To remove the IP address interface configuration, use the **no** form of this command.

ip address *ip-address network-mask*

no ip address

Syntax Description

ip-address	Configures the IP address.
network-mask	Configures the network mask.

Defaults

None.

Command Default

None.

Command Modes

Cisco AXP interface configuration.

Command History

Cisco AXP 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

In the following example, the IP address of an interface in Cisco AXP interface configuration mode is specified:

```
se-Module (config-interface)> ip address 209.165.201.1 255.255.255.224
```

Related Commands

Command	Description
interface	Configures the interface device.

ip domain-name

To configure the domain name for the application, use the **ip domain-name** command in Cisco AXP application configuration mode.

To disable the domain name, use the **no** form of this command.

ip domain-name ***dns-server-domain-name***

no ip domain-name

Syntax Description

dns-server-domain-name	Domain name for the DNS server.

Defaults

No domain name is configured.

Command Default

None.

Command Modes

Cisco AXP application service configuration.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

The domain-name is limited to 64 characters.

If you enter more than 64 characters, the following error message appears:

Error Message `domain size greater than 64`

This command modifies configuration directives in */etc/hosts* and */etc/resolv.conf* files where the domain name is relevant, and also modifies the search list for hostname lookup and domain directives for local domain name in the */etc/resolv.conf* file.

For the */etc/hosts* file, this command updates the domain name of the hostname-ip mapping entry.

Example:

```
/etc/resolv.conf:
search cisco.com    ## added by cli
domain cisco.com    ## added by cli
nameserver x.x.x.x  ## added by cli

/etc/hosts:
10.100.50.10 appre.cisco.com appre
```

Use this command with the **ip name-server** command to configure the DNS server. The host commands **ip domain-name** and **ip name-server** populate the */etc/resolv.conf* file in each installed virtual instance. Changing the configuration results in the updating of host results in the */etc/resolv.conf* file.

When these commands are used to configure a new name-server and domain-name for a virtual instance (in app-service mode), the */etc/resolv.conf* file in that virtual instance is overridden with the new server name and domain name.

The */etc/resolv.conf* file in that virtual instance reverts to the host configuration whenever the virtual instance does not have a name-server or domain-name configured.

Configuring the name-server and domain-server in a virtual instance always takes precedence over configuration in the host.

Examples

In the following example, the domain name of the application is changed from **mping** to **mycompany.com**:

```
SE-Module> config t
se-Module(config-mping)> ip domain-name mycompany.com
se-Module(config-mping)> ip name-server 10.0.61.1
```

Related Commands

Command	Description
hostname	Specifies the server that stores the Cisco AXP applications.
ip name-server	Specifies the DNS server name of the application.
ntp server	Specifies the NTP clocking server.
show hosts	Displays all configured hosts.
show ip route	Displays IP route destinations, gates, and masks.

ip local policy route-map

To configure a route map for policy routing, use the **ip local policy route-map** command in Cisco AXP configuration mode.

To remove the IP local policy configuration, use the **no** form of this command.

ip local policy route-map *map-tag*

no ip local policy route-map

Syntax Description

map-tag	Route map name.

Defaults

None.

Command Default

None.

Command Modes

Cisco AXP configuration.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

The route map name must match the *map-tag* in the **route-map** command.

Examples

In the following example, the route map is configured for policy routing with *map-tag*=10:

```
se-Module(config)> ip local policy route-map 10
```

Related Commands

Command	Description
route map	Specifies the route map.

ip name-server

To configure the IP address of the domain name server (DNS) of the application, use the **ip name-server** command in Cisco AXP application service configuration mode.

To disable the name server, use the **no** form of this command.

ip name-server ***ip-address***

no ip name-server

Syntax Description

ip-address	IP address of the DNS server.

Defaults

No name server is configured.

Command Default

None.

Command Modes

Cisco AXP application service configuration.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command with the **ip domain-name** command to configure the DNS server. A maximum of two DNS servers can be defined. In a Linux environment, the */etc/resolv.conf* file typically contains the IP addresses of name servers (DNS name resolvers) that attempt to translate names into addresses for any node available on the network.

The **ip domain-name** and **ip name-server** commands in the host populate the */etc/resolv.conf* file in each installed virtual instance. Using this command to change the configuration in the host results in the */etc/resolv.conf* file being updated.

When these commands are used to configure a new name-server and domain-name for a virtual instance (in app-service mode), the */etc/resolv.conf* file in that virtual instance is overridden with the new server name and domain name.

The */etc/resolv.conf* file in that virtual instance reverts back to the host configuration whenever the virtual instance does not have a name-server or domain-name configured. Configuring the name-server and domain-server in a virtual instance always takes precedence over configuration in the host.

If an application package has already bundled its own */etc/resolv.conf* file, the new entries will be appended to the existing ones and will leave the original ones intact.

Example:

```
search localdomain## added by cli
domain localdomain## added by cli
nameserver x.x.x.x## added by cli
```

Examples

In the following example, the IP name server of the application is changed from mping to 10.10.61.16:

```
se-Module> config t
se-Module(config-mping)> ip name-server 10.10.61.16
se-Module(config-mping)> ip domain-name mycompany.com
```

Related Commands

Command	Description
hostname	Specifies the server that stores the Cisco AXP applications.
ip domain-name	Specifies the DNS domain name of the application.
ntp server	Specifies the NTP clocking server.
show hosts	Displays all configured hosts.
show ip route	Displays IP route destinations, gates, and masks.

ip route

To configure a static IP route, use the **ip route** command in Cisco AXP configuration mode.

To remove the static IP route configuration, use the **no** form of this command.

ip route {*dest-prefix dest-mask forwarding-address* | **table** *dest-prefix dest-mask forwarding-address*}

no ip route {*dest-prefix dest-mask forwarding-address* | **table** *table-num dest-prefix dest-mask forwarding-address*}

Syntax Description

dest-prefix	Sets the static IP route destination prefix address.
dest-mask	Sets the static IP route destination mask.
forwarding-address	Sets the forwarding router address.
table	Establishes the IP route using multiple routing table.
table-num	Route table number in the range of 1 to 252.

Defaults

None.

Command Default

None.

Command Modes

Cisco AXP configuration.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to configure an IP static route or table for a connected route.

Examples

In the following example, the static IP route is configured using the destination prefix 10.0.0.0, destination prefix mask 255.255.255.0, and the forwarding router's address 172.16.0.0:

```
se-Module (config)> ip route 10.0.0.0 255.255.255.0 172.16.0.0
```

Related Commands

Command	Description
show ip route	Displays the main routing table for all configured IP routes.

ip route table

To configure the IP route table for a connected route, use the **ip route table** command in Cisco AXP interface configuration mode.

To remove the route table, use the **no** form of this command.

ip route table *table-num*

no ip route table *table-num*

Syntax Description

table-num	Route table number from 1 to 100.

Defaults

None.

Command Default

None.

Command Modes

Cisco AXP interface configuration.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to configure the route table for a connected route for source-based routing.

Examples

In the following example, the route table number 10 is configured:

```
se-Module (config-interface)> ip route table 10
```

Related Commands

Command	Description
interface	Configures the interface device.
ip address	Configures the IP address for the specified network interface.

ip ssh interface

To enable the interface on which the sshd daemon (SSH) listens for an incoming connection, use the **ip ssh interface** command in Cisco AXP configuration mode.

To remove the SSH interface configuration, use the **no** form of this command; the sshd process then listens ro all interfaces.

ip ssh interface

no ip ssh interface *interface*

Syntax Description

interface	Interface name.

Defaults

None.

Command Default

None.

Command Modes

Cisco AXP configuration.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

This command specifies the interface on which the sshd process listens for an incoming connection. If you do not specify this command, the sshd process listens on all interfaces.

Related Commands

Command	Description
ip ssh server	Configures the SSH server.

ip ssh server

To enable the IP SSH service, use the **ip ssh server** command in Cisco AXP application configuration mode.

To disable the service, use the **no** form of this command.

ip ssh server

no ip ssh server

Syntax Description

This command has no arguments or keywords.

Defaults

Port number 22.

Command Default

Enabled.

Command Modes

Cisco AXP syslog application service configuration.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to start or stop the SSH server. The default port number is 22.

Error messages: Table

Error Message	Description
Port is in use, please use another port.	System cannot start the SSH server because the port designated with number *port-num* is currently being used. After seeing this message, you can re-enter the command, using a different value for *port-num*.
Invalid port number, range is 1-65535	Invalid port number entered.

Examples

In the first of the following examples, the IP SSH server is enabled.

```
se-Module(config)> ip ssh server
```

The second example disables the IP SSH server.

```
se-Module(config)> no ip ssh server
```

Related Commands

Command	Description
ip ssh interface	Interface on which the sshd daemon listens for an incoming connection.

ip ssh username

To specify an unencrypted or hidden password for SSH tunneling, use the **ip ssh username** command in Cisco AXP syslog application configuration mode.

To disable tunneling, use the **no** form of the command.

ip ssh username [tunnel_root | tunnel_user] password *clear-password-string*

no ip ssh username [tunnel_root | tunnel_user] password *clear-password-string*

Syntax Description

tunnel_root	Allows an SSH user with shell access to the application environment.
tunnel_user	Allows an SSH user shell access to the application environment through a startup script that is implemented by the third party developer.
clear-password-string	UNIX password for the user with a minimum of five characters.

Defaults

None.

Command Default

None.

Command Modes

Cisco AXP syslog application service configuration.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

For a tunnel user, the startup script decides on the level of access a user can have to perform specific operations.

Related Commands

Command	Description
ip ssh interface	Specifies the interface on which the sshd daemon listens for an incoming connection.

limit cpu utilization

To configure the CPU resource usage limits, use the **limit cpu utilization** command in Cisco AXP application service configuration mode.

To disable setting CPU utilization limits, use the **no** form of this command.

limit cpu utilization *index*

no limit cpu utilization *index*

Syntax Description

index	CPU index number.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP application service configuration.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

This command modifies the CPU utilization limit when the application is installed. It becomes effective when the application instance restarts.

The CPU utilization range varies between the minimum and maximum limits specified by the package. The specified CPU utilization maximum for a Cisco AXP service module is based on a platform CPU index.

The platform CPU index is specified relative to a value of 10000 assigned to the following configuration: 1.0 GHz Celeron M CPU on the application runtime engine of an NME_APPRE_302-K9 network module. For example, the CPU utilization limit for the AIM_APPRE 102 blade is 3000.

Examples

In the following example, the CPU utilization limit is set to 3000, (typical for an AIM_APPRE 102 blade):

```
se-Module(config-helloworld)> limit cpu utilization 3000
```

Related Commands

Command	Description
show resource limits	Displays the resource limits configured for the application.

limit disk utilization

To modify the disk utilization setup during installation, use the **limit disk utilization** command in Cisco AXP application service configuration mode.

To disable setting of disk utilization limits, use the **no** form of the command.

limit disk utilization *amount*

no limit disk utilization *amount*

Syntax Description

amount	Range is 1 to 100,000 MB

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP application service configuration.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

This command limits the disk space utilization in a virtual instance. The disk utilization range varies between the minimum limit specified by the package to the maximum limit available to the system.

Examples

In the following example, the disk utilization is set to 100 MB during installation:

```
se-Module(config-myapp1)> limit disk utilization 100
```

Related Commands

Command	Description
show resource limits	Displays the resource limits configured for the application.

limit log-file size

To configure the log file size, use the **limit log-file size** command in Cisco AXP application service configuration mode.

To disable log file size configuration, use the **no** form of this command.

limit log-file size *size*

no limit log-file size *size*

Syntax Description

size	Maximum log file size in MB. Range is 0 to 40 MB.

Defaults

Default value is 5 MB.

Command Default

None.

Command Modes

Cisco AXP application service configuration.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

This command sets the maximum size of the log file /var/log/*messages.log*. Each virtual instance writes a syslog to its own file */var/log/messages.log*. When this file reaches the limit specified by this command, its contents are moved to a backup log file *messages.log.prev* and a new *messages.log* file is started. The range is 0–40 MB with a default size of 5 MB for two files.

megabytes: The range of the log file size from 0–40 MB.

When the value is out of range, the following message appears:

```
%Invalid input detected at '^' marker
```

If the log file size configuration is disabled (**no limit log-file size**), the maximum size of the log file reverts to the default value of 5 MB.

If the maximum size of the log file is set to 0 MB, the minimum file size is 10 KB.

Examples

In the following example, the size of the log file is changed to 10 MB.

```
se-Module(config-helloworld)> limit log-file size 10
```

Related Commands

Command	Description
show logs	Lists logs in the application environment that reside in the /var/log directory.

limit memory utilization

To modify the memory utilization setup during installation, use the **limit memory utilization** command in Cisco AXP application service configuration mode.

To disable settings of memory utilization limits, use the **no** form of the command.

limit memory utilization *nn*

no limit memory utilization *nn*

Syntax Description

nn	Memory utilization in Megabytes

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP application service configuration.

Command History

Cisco AXP Version	Modification
1.1	This command was introduced.

Usage Guidelines

This command limits the memory utilization in a virtual instance. The disk utilization range varies between the minimum limit specified by the package to the maximum limit available to the system.

Examples

In the following example, the memory utilization is set to 100 MB during installation:

```
se-Module(config-demo)> limit memory utilization 100
```

Related Commands

Command	Description
show resource limits	Displays the resource limits configured for the application.

log console

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

log console {**errors** | **info** | **notice** | **warning**}

no log console {**errors** | **info** | **notice** | **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 may be difficult. Pressing CTRL-c does not work for this command.

Syntax Description

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

Defaults

Only fatal error messages are displayed.

Command Modes

CiscoAXP configuration

Command History

Cisco AXP Release	Modification
1.0	This command was introduced.

Usage Guidelines

The messages on the console display are also saved in the messages.log file. These messages can be used for debugging purposes.

Examples

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

```
se-Module> config t
se-Module(config)> log console errors
se-Module(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 Cisco AXP 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 may be difficult. Pressing CTRL-c does not work for this command.

Syntax Description

module	Cisco AXP modules.
entity	Cisco AXP module entities.
activity	Cisco AXP entity actions.

Defaults

Only fatal error messages are displayed.

Command Modes

Cisco AXP EXEC

Command History

Cisco AXP Release	Modification
1.0	This command was introduced.

Usage Guidelines

The messages on the console monitor are also saved in the messages.log file. These messages can be used for debugging purposes.

Examples

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

```
se-Module> log console monitor networking database results
```

Related Commands

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

log trace boot

To save the trace configuration upon rebooting, use the **log trace boot** command in Cisco AXP EXEC mode.

log trace boot

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco AXP EXEC

Command History

Cisco AXP Release	Modification
1.0	This command was introduced.

Usage Guidelines

To ensure that the current trace configuration is saved when the Cisco AXP service module is rebooted, use the **log trace boot** command.

Examples

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

```
se-Module>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 Cisco AXP EXEC mode.

log trace buffer save

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco AXP EXEC

Command History

Cisco AXP Release	Modification
1.0	This command was introduced.

Usage Guidelines

Current trace information stored in the memory buffer can be saved to a file.

Examples

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

```
se-Module>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.

log trace local enable

To configure tracing messages to a local disk, use the **log trace local enable** command in Cisco AXP configuration mode.

log trace local enable

Syntax Description

There is no syntax description for this command.

Defaults

None

Command Modes

Cisco AXP configuration

Command History

Cisco AXP Release	Modification
1.0	This command was introduced.

Usage Guidelines

Enable local tracing to a disk.

Examples

The following example configures tracing to a local disk:

```
se-Module> config t
se-Module(config)> log trace local enable
se-Module(config)> exit
```

Related Commands

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

log trace server

To configure tracing messages for remote storage, use the **log trace server** command in Cisco AXP configuration mode.

log trace server {enable | url *url*}

Syntax Description

enable	Enables tracing to the FTP server.
url	Designates remote storage directory.
url	FTP URL address.

Defaults

None

Command Modes

Cisco AXP configuration

Command History

Cisco AXP Release	Modification
1.0	This command was introduced.

Usage Guidelines

Configures tracing messages for remote storage.

Examples

The following example configures tracing remotely:

```
se-Module> config t
se-Module(config)> log trace server url ftp url
se-Module(config)> exit
```

Related Commands

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

log server address

To configure the remote logging server, use the **log server address** command in Cisco AXP application service configuration mode.

To disable the remote logging server, use the **no** form of this command.

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

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

Syntax Description

ip-address	IP address of the external log server.
hostname	Hostname of the external log server.

Defaults

No external log server is configured.

Command Modes

Cisco AXP application service configuration.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced

Usage Guidelines

This command enables and disables remote logging, and configures the remote logging server. Application syslog messages are sent to the specified log server. The hostname can be an IP address or a name.

When an invalid IP address format such as 0.0.0.0 is entered, the following error message appears:

Error Message `0.0.0.0 is an invalid Host IP address`

This is used to stream out the application logs to the remote syslog server.

Examples

In the following example, IP address 10.1.61.16 is assigned as the external log server:

```
se-Module(config-mping)> log server address 10.1.61.16
se-Module(config-mping)> exit
```

Related Commands

Command	Description
show hosts	Displays all configured hosts.
show log	Displays a specific log.
show logs	Displays all logs.
show running-config	Displays the log server as part of the configuration.

log level

To configure the different system log levels, use the **log level** command in Cisco AXP application service configuration mode.

To disable log levels, use the **no** form of this command.

log level *levels*

no log level *levels*

Syntax Description

levels	**info:** Events with LOG_INFO and higher severity are logged, including all messages described in **notice**. **warn** (Default): Events with LOG_WARNING and higher severity are logged, including all error messages described in **err**. **err**: Events with LOG_ERR and higher severity are logged, including LOG_EMERG, LOG_ALERT, and LOG_CRIT. **notice**: Events with LOG_NOTICE and higher severity are logged, including all messages described in **warn**. **debug** – Events with LOG_DEBUG and higher severity are logged, including all messages described in **info**.

Defaults

warn is the default value.

Command Default

None.

Command Modes

Cisco AXP application service configuration.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

The following example shows the log level being set so that events with LOG_INFO or higher severity are logged:

```
se-Module(config-myapp)> log level info
```

Usage Guidelines

log level info logs events with LOG_INFO or higher severity.

In the following example, events within the stdout of a CLI plug-in and the output from System.out.println calls made by the application MyAppMain, are redirected to syslog if they have a log level of LOG_INFO or above.

```
# java -cp
./app_bin/myApp.jar:/cli_comm/:/usr/lib/java/localsocket.jar:/usr/lib/java/cli_distributio
n_vm.jar com.myApp.MyAppMain | /bin/logger -p info
```

Related Commands

Command	Description
show log	Displays a specific log.
show logs	Displays all logs.

netconf

To configure the Network Configuration Protocol (NETCONF), use the **netconf** command in Cisco AXP configuration mode.

To remove the NETCONF configuration, use the **no** form of this command.

netconf {beep *initiator* {*hostname* | *ip-address*} *dest-port* | **max-sessions** *max-sessions*}

no netconf {beep *initiator* {*hostname* | *ip-address*} *dest-port* | **max-sessions** *max-sessions*}

Syntax Description

beep	Set to use Blocks Extensible Exchange Protocol (BEEP) transport.
initiator	Configure NETCONF initiator parameters.
hostname	Set hostname of destination network device.
ip-address	Set IP address of destination network device.
dest-port	Set port number of destination device in the range of 1 to 65535.
max-sessions	Configure maximum number of NETCONF sessions between server and client.
max-sessions	Set maximum number of NETCONF sessions in the range of 1 to 16.

Defaults

None

Command Modes

Cisco AXP configuration

Command History

Cisco AXP Release	Modification
1.0	This command was introduced.

Usage Guidelines

The NETCONF over BEEP feature must be configured on the router and the Cisco AXP service module. NETCONF over BEEP in Cisco IOS software does not support any authentication. It supports only an SASL/Anonymous profile.

The NETCONF over BEEP feature allows you to enable either the NETCONF server or the NETCONF client to initiate a connection. This supports large networks of intermittently connected devices and those devices that must reverse the management connection where firewalls and network address translators (NATs) exist.

The Network Configuration Protocol (NETCONF) defines a simple mechanism through which a network device can be managed, configuration data information can be retrieved, and new configuration data can be uploaded and manipulated. NETCONF uses Extensible Markup Language (XML)-based data encoding for the configuration data and protocol messages.

Blocks Extensible Exchange Protocol (BEEP) can use the Simple Authentication and Security Layer (SASL) profile to provide simple and direct mapping to the existing security model. Alternatively, NETCONF over BEEP can use the transport layer security (TLS) to provide a strong encryption mechanism with either server authentication or server and client-side authentication.

NETCONF over BEEP sends notifications of any configuration change over NETCONF. A notification is an event indicating that a configuration change has happened. The change can be a new configuration, deleted configuration, or changed configuration. The notifications are sent at the end of a successful configuration operation as one message showing the set of changes, rather than individual messages for each line in the configuration that is changed.

Examples

The following example configures tracing remotely:

```
se-Module> config t
se-Module(config)> netconf max-sessions 16
se-Module(config)>
```

Related Commands

Command	Description
show netconf session	Displays the current number of netconf sessions.

ntp server

To synchronize the Cisco AXP application system clock with a remote Network Time Protocol (NTP) server, use the **ntp server** command in Cisco AXP configuration mode.

To disable the Cisco AXP 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

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

Defaults

The default is the IP address of the server.

Command Default

None.

Command Modes

Cisco AXP configuration.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command in conjunction with the **clock time** command to set the timing functions for Cisco AXP 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-Module(config)> ntp server 192.168.1.100 prefer
```

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

```
se-Module(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.

reload apps

To apply new resource limits without rebooting the service module, use the **reload apps** command in Cisco AXP EXEC mode.

reload apps

Syntax Description

There are no arguments for this command.

Defaults

None

Command Modes

Cisco AXP EXEC

Command History

Cisco AXP Release	Modification
1.1	This command was introduced.

Usage Guidelines

Use the **reload apps** command after configuring the new resource limits and executing the **write memory** command.

Related Commands

Command	Description
limit memory utilization	configures memory limits.
limit cpu utilization	Configures CPU limits.
limit disk utilization	Configures disk capacity limits.

reset

To reset the hosting envirnment, use the **reset** command in Cisco AXP EXEC mode.

reset

Syntax Description

There are no arguments for this command.

Defaults

None

Command Modes

Cisco AXP EXEC

Command History

Cisco AXP Release	Modification
1.0	This command was introduced.

Usage Guidelines

Use the **reset** command reset the application services hosting environment.

Related Commands

Command	Description
show app-service state	Displays all the installed services applications.
show app-service statistics	Displays the statistical data of all the installed services applications.
show app-service status-monitor	Displays the status monitor of all the installed services applications.

route-map

To configure the route map, use the **route-map** command in Cisco AXP configuration mode.

To remove the route map, use the **no** form of this command.

route-map *name sequence-num*

no route-map *name sequence-num*

Syntax Description

name	Name of route map.
sequence-num	Route map sequence number in the range of 1 to 99.

Defaults

None

Command Modes

Cisco AXP configuration

Command History

Cisco AXP Release	Modification
1.0	This command was introduced.

Usage Guidelines

This command configures the route map name and sequence number parameters.

Route maps are identified by a map name. You can assign the route map name when the route map is created. It can be composed of multiple lines, each with a sequence number in the range of 1 to 99, where each line can have multiple match and set commands. An incoming packet is compared to each line of the route map until there is a match, then the set actions for that line are applied to the packet similar to the way an access list is applied. The last line of a route-map is an implicit deny.

Examples

The following example configures tracing remotely:

```
se-Module> config t
se-Module(config)> route-map test 45
se-Module(config-route-map)>
```

Related Commands

Command	Description
show route-map	Displays the route-map.

service password-encryption

To enter the password encryption mode, use the **service password-encryption** command in Cisco AXP configuration mode.

To exit the password encryption mode, use the **no** form of this command.

service password-encryption

no service password-encryption

Syntax Description

There are no arguments for this command.

Defaults

None

Command Modes

Cisco AXP configuration

Command History

Cisco AXP Release	Modification
1.0	This command was introduced.

Usage Guidelines

Use the **service password-encryption** command to enter the password encryption mode.

Related Commands

Command	Description
show running-config	Displays the content of the current running configuration.
show startup-config	Displays the content of the startup configuration.

status-monitor

To configure the status monitor and recovery threshold, use the **status-monitor** command in Cisco AXP application service configuration mode.

status-monitor monitor_interval *Interval-Num* **recovery_threshold** *Threshold-Num*

Syntax Description

monitor_interval	Threshold value for monitoring interval.
Interval-Num	Range is 1 to 99. Default is 12. Measured at 5 seconds per interval.
recovery_threshold	Threshold value for recovery attempts.
Threshold-Num	Recovery threshold range is 1 to 99. Default is 5.

Defaults

Default value for monitor interval is 12 and recovery threshold is 5.

Command Default

None.

Command Modes

Cisco AXP application service configuration.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

Cisco AXP allows third party applications to plug in their status monitoring and allows recovery from a malfunctioned state.

An application must provide one or more watchdog scripts or executable files bundled in their package to use the Cisco AXP application monitoring feature. The number of scripts or executables is dependent on the application, resulting in a unique way of determining the status of the application. For example, it can be based on Process Identifier (PID), or a response to an application ping. Cisco AXP supports Shell scripts and C language executables for application status monitoring.

For more information on watchdog scripts and executables, see the *Cisco AXP Developer Guide*.

The application status monitor has a heartbeat of 5 seconds, which is the minimum interval used for monitoring. For example, if the monitor interval is set at 12, monitoring of each virtual instance takes place every 12 heartbeat intervals, which is every one minute. You can configure the monitoring interval for a virtual instance through the **status-monitor monitor interval** command.

The scripts or executables return a status code where zero indicates that the application is healthy and alive. A non zero status code indicates that the application is not functional. When a watchdog script or executable returns a non zero status code, relevant information such as the name of the watchdog script, return status, and time of failure is logged.

A recovery counter counts the number of times the failure takes place, and acts as a delay mechanism for further action. A recovery count of three means that the application monitor has run for three iterations and is receiving either a non zero return status, or the watchdog script has been running for over 3 monitoring intervals and is not returning a value.

You can use the **status-monitor monitor interval** command for configuring the recovery threshold that decides on the number of recovery counters before taking the next action. When the recovery threshold is reached, the virtual instance restarts and the application monitor continues to run, repeating the monitoring cycle. A virtual instance can restart any number of times.

If you are developing a third party application, you can provide default configuration parameters using a configuration file that is packaged together with the application.

Examples

The following example sets the threshold value for the monitor interval to 10 (monitoring occurs every 50 seconds) and the threshold value for recovery attempts to 10.

```
se-Module(config-mping)> status-monitor monitor_interval 10 recovery_threshold 10
```

Related Commands

Command	Description
show status-monitor	Displays data for the application status monitor.

show app-service state

To display the state and health of all installed virtual instances and applications, use the **show app-service state** command in Cisco AXP EXEC mode.

show app-service state

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command frequently on the application service module to determine whether your applications are up and running.

Examples

In the following example, for each of three running applications, the application's name, state, and health are displayed on the screen.

```
se-Module> show app-service state
                  APPLICATION                 STATE                HEALTH
                   helloworld                online                 ALIVE
              simpleFC4CPlusApp                online                   ---
                        x11_app                online                   ---
```

Related Commands

Command	Description
show app-service state	Displays the status and health of a specific application in Cisco AXP application service EXEC mode.

show app-service statistics

To display the memory and processing time information of an installed virtual instance, use the **show app-service statistics** command in Cisco AXP EXEC mode.

show app-service statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, the statistics for all installed virtual instances are displayed on the screen.

```
se-Module> show app-service statistics
CTX   PROC    VSZ    RSS  userTIME   sysTIME    UPTIME NAME
0      122   2.7G 626.9M   1h23m20   1h39m08   6d18h56 root server
2        4   8.6M   2.9M   1m46s57   2m07s88   6d18h54 helloworld
CTX = context number for the virtual instance
PROC = quantity of processes in the context
VSZ = number of pages of virtual memory
RSS = Resident set size limits for memory
userTime = utime User-mode CPU time accumulated
sysTime = ctime Kernel-mode CPU time accumulated
upTime = uptime
```

Related Commands

Command	Description
show app-service statistics	Allows third party applications to integrate their own application statistics for display.

show app-service status-monitor

To display status monitor information for all installed applications, use the **show app-service status-monitor** command in Cisco AXP EXEC mode.

show app-service status-monitor

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, the monitoring information for helloworld is displayed on the screen. (helloworld is the only installed application.)

```
se-Module> show app-service status-monitor
Application: helloworld
Monitor status: PASSED
Monitor in progress: Yes
Last executed watchdog: W00template.sh
Last executed date: Wed Sep  5 14:09:58 PDT 2007
Last failed watchdog: ---
Last failed return code: -
Last failed date: ---
Last restarted date: ---
Recovery threshold: 4
Monitor interval: 3
```

Related Commands

Command	Description
show app-service status-monitor	Displays the application service status.
show running-config	Displays the current running configuration.

show arp

To display the ARP table, use the **show arp** command in Cisco AXP EXEC mode.

show arp [|]

Syntax Description

|	(Optional) Pipe output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, the ARP table is displayed.

```
se-Module> show arp
Address                  HWtype  HWaddress           Flags Mask            Iface
1.100.30.150             ether   00:1E:7A:E1:41:B8   C                     eth0
```

Related Commands

Command	Description
show interfaces	Displays all the interfaces configured on the Cisco AXP module.

show clock detail

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

show clock [**detail** | **|**]

Syntax Description

detail	(Optional) Display clock configuration details.
|	(Optional) Pipe output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

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

```
se-Module> show clock detail
se-Module> 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 timezone.
ntp server	Configures the NTP server for time synchronization

show configuration

To display non-volatile memory (NVRAM) configuration, use the **show configuration** command in Cisco AXP EXEC mode.

show configuration [**paged** | |]

Syntax Description

paged	(Optional) Displays enough output to fill the current viewing screen.
|	(Optional) Pipe output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, the NVRAM configuration displayed on the screen.

```
se-Module> show configuration
!
! This adds all the platform CLI commands
!

! host name
hostname se-1-100-30-151

! domain name
ip domain-name localdomain

! DNS Servers
!VAR_DNS_SERVER

! Timezone Settings
clock timezone America/Los_Angeles

! NTP Servers
ntp server 1.100.30.150 prefer
```

```
end
```

Related Commands

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

show cores

To display a list of core files, use the **show cores** command in Cisco AXP EXEC mode.

show cores [|]

Syntax Description

|	(Optional) Pipe output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, the **show cores** command displays a list of the core files.

```
se-Module> show cores
     SIZE             LAST_MODIFIED_TIME                                NAME
```

Related Commands

Command	Description
copy core	Copies core file to another location.

show crash buffer

To display the recent kernel crash log, use the **show crash buffer** command in Cisco AXP EXEC mode.

show crash buffer [|]

Syntax Description

|	(Optional) Pipe output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, there was no recent crash of the kernel so that the **show crash buffer** command does not display the crash buffer contents.

```
se-Module> show crash buffer
Press <CTRL-C> to exit...
```

Related Commands

Command	Description
clear crashbuffer	Clears the kernel crash buffer.

show debugging

To display the state of each debugging option, use the **show debugging** command in Cisco AXP EXEC mode.

show debugging [|]

Syntax Description

|	(Optional) Pipe output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, there was no recent debug activity, so that the **show debug** command does not display the trace results.

```
se-Module> show debugging
Debug Logging Info:

MODULE           ENTITY          ACTIVITY

No debug active
```

Related Commands

Command	Description
trace all	Enables trace events for debugging.

show device serial

To display the serial device ID, use the **show device serial** command in Cisco AXP EXEC mode.

show device serial

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Default

None

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, all the serial devices are displayed on the screen.

```
se-Module> show device serial
Device Name     TTY No. Line No.   Line Type    Intf Name  Assigned To
vaux1           1       1            AUX        -              -
vtty000         0/0/0   2            TTY        Se0/0/0        serialapp
vtty001         0/0/1   3            TTY        Se0/0/1        -
```

Related Commands

Command	Description
bind serial	Binds the serial device.

show errors

To display error statistics by module, entity, or activity, use the **show errors** command in Cisco AXP EXEC mode.

show errors [|]

Syntax Description

|	(Optional) Pipe output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Defaults

None

Command Modes

Cisco AXP EXEC

Command History

Cisco AXP Release	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command with the **show log name** command to narrow down error statements.

Examples

The following example shows the result of the **show errors** command.

```
se-Module> show errors
Module error report:
MODULE           ENTITY           ACTIVITY         NUM ERRORS
Startup          Capabilities     cap_include.sh      4
```

Related Commands

Command	Description
show log name	Displays a specific log file in the application environment.

show history iosapi

To display the IOS service API historical records, use the **show history iosapi** command in Cisco AXP EXEC mode.

show history iosapi [*num-records* | **config** *num-records* | **exec** *num-records*]

Syntax Description

num-records	(Optional) Display the total number of history records in the range of 1 to 100.
config *num-records*	(Optional) Display the following number of configuration mode history records in the range of 1 to 70.
exec *num-records*	(Optional) Display the following number of EXEC mode history records in the range of 1 to 30.

Defaults

None

Command Modes

Cisco AXP EXEC

Command History

Cisco AXP Release	Modification
1.0	This command was introduced.

Usage Guidelines

The Cisco IOS Service API allows you to write applications that access router information and change system configurations using commands equivalent to Cisco IOS configuration and AXP EXEC mode commands.

Use this command to view the historical records of the IOS API.

Related Commands

Command	Description
show app-service state	Displays a list of the installed service applications.

show hosts

To display IP domain-name, lookup style, nameservers, and host table, use the **show hosts** command in Cisco AXP EXEC mode.

show hosts [|]

Syntax Description

|	(Optional) Pipe output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Defaults

None

Command Modes

Cisco AXP EXEC

Command History

Cisco AXP Release	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command with the **show log name** command to narrow down error statements.

Examples

The following example shows the result of the **show hosts** command.

```
se-Module> show hosts
Hostname:      se-1-100-30-151
Domain:        localdomain
```

Related Commands

Command	Description
show running-config	Displays the content of the current running configuration.

show interfaces

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

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

Syntax Description

GigabitEthernet	Gigabit Ethernet IEEE 802. device.
ide	Integrated Drive Electronics (hard disk)
|	Pipes output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP 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 GigabitEthernet interface and an IDE (hard disk) interface.

```
se-Module> 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 ip access-list

To display IP access list information, use the **show ip access-list** command in Cisco AXP EXEC mode.

show ip access-list [*acl-name* | *acl-num* | **details**]

Syntax Description

acl-num	Numeric identifier in the range of 1 to 99 for an access list to which all commands entered in access list configuration mode apply.
acl-name	Name identifier for an access list to which all commands entered in access list configuration mode apply. Format: 30 alphanumeric characters, beginning with a letter.
details	Display the IP table information.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, the **show ip access-list 10** command displays the access list identified by the number 10.

```
se-Module> show ip access-list 101
```

Related Commands

Command	Description
ip access-list standard	Configures standard IP access lists.

show ip route

To display the static IP route information, use the **show ip route** command in Cisco AXP EXEC mode.

show ip route [|]

Syntax Description

|	(Optional) Pipe output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, the **show ip route** command displays the IP route information.

```
se-Module> show ip route
Main Routing Table:
           DEST            GATE             MASK IFACE
     1.100.30.0         0.0.0.0  255.255.255.0 eth0
        0.0.0.0   1.100.30.150        0.0.0.0 eth0
```

Related Commands

Command	Description
ip route	Configures static IP routes.

show license udi

To view the unique device identifier (UDI) of the service module, use the **show license udi** command in Cisco AXP EXEC mode.

show license udi

Syntax Description

There are no arguments for this command.

Defaults

None

Command Modes

Cisco AXP EXEC

Command History

Cisco AXP Release	Modification
1.1	This command was introduced.

Usage Guidelines

Each Cisco AXP service module contains a unique device identifier (UDI) that must be used by customers when they contact their Cisco marketing representative for unrestricted shell access.

The UDI consists of the following sequence:

1. The service module's PID
2. A colon (**:**)
3. The service module's serial number

Examples

Step 1 Retrieve UDIs using the **show license udi** command:

show license udi: Example 1

In this example, the command is run on a network module.

```
show license udi
PID            SN              UDI
--------------------------------------------------
AIM-CUE        FOC10222W1M     AIM-CUE:FOC10222W1M
```

show license udi: Example 2

In this example, the command is run on PC 104 hardware or VMware.

```
show license udi
PID            SN              UDI
--------------------------------------------------
AIM-CUE        -- AIM-CUE:FOC10222W1M
```

show log name

To display a specific log file in the application environment, use the **show log name** command in Cisco AXP application service EXEC mode.

To display system-level logging data for a specific log file, use the **show log name** command in Cisco AXP EXEC mode.

show log name *log-name* {**containing** *expression* | **paged** | **interactive** | {|**begin** | |**exclude** | |**include** [*string* | *module*] | |**page**} | **tail**}

Syntax Description

log-name	Log name. See the **show logs** command for log names.
containing *expression*	Displays events matching a regular expression (regex) pattern, where *expression* is a regex.
paged	(Optional) Displays enough output to fill the current viewing screen.
interactive	Displays logs in interactive mode.
|**begin** *string*	Checks if string begins the line and pipes output to another command.
|**exclude** *string*	Checks if string is not included in the line and pipes output to another command.
|**include** *string*	Checks is string is included in the line and pipes output to another command.
string	A literal that can be an ERROR or INFO message.
module	Defines a logging or tracing module (see Table 1).
|**page**	Pipes output to another command and paginates the output.
tail	Waits for events and prints them as they occur.

Table 1 Logging Module Definitions

AXP_install	AXP_upgrade
AXP_startup	AXP_rsrcmgr
AXP_cliapi	AXP_ssh
AXP_snmp	AXP_syslogsvr
AXP_cli	AXP_cliplugin
AXP_appdebug	AXP_guestos
AXP_vserial	AXP_iosapi
AXP_eemapi	

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP application service EXEC.

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

show logging

To display the console logging options, use the **show logging** command in Cisco AXP EXEC mode.

show logging [|]

Syntax Description

|	(Optional) Pipe output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, the **show logging** command displays the console logging options.

```
se-Module> show logging
info:     off
notice:   off
warning:  off
errors:   off
fatal:    on

Monitored event  Info:

MODULE           ENTITY           ACTIVITY        FILTER

No monitored events active

Server Info:

Log server address:
```

Related Commands

Command	Description
show log name	Displays system-level logging data for a specific log file.
show logs	Displays log files on the Cisco AXP service module.

show logs

The **show logs** command can be used in either of the following two modes:

- Cisco AXP application service EXEC mode: the command displays log files in the application environment.

  show logs

- Cisco AXP EXEC mode: the command displays log files on the Cisco AXP service module.

  show logs [|]

Syntax Description

|		(Optional) For Cisco AXP EXEC mode, used to pipe output to another command.
	begin	(Optional) Display begins with the line that matches.
	exclude	(Optional) Display excludes lines that match.
	include	(Optional) Display includes lines that match.
	page	(Optional) Displays paginated output (--More--).

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP application service EXEC.

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

In Cisco AXP application service EXEC mode, this command displays all the log files under the /var/log directory of the virtual instance.

Examples

In the following example, the **show logs** command, executed in Cisco AXP application service EXEC mode, shows the log files under the /var/log directory of the virtual instance.

```
se-Module(exec-mping)> show logs
SIZE    LAST_MODIFIED_TIME              NAME
108     Mon Nov 05 19:50:33 PST 2007    messages.log
```

In the following example, the **show logs** command, executed in Cisco AXP EXEC mode, shows the log files on the Cisco AXP service module.

```
se-Module> show logs
```

```
SIZE            LAST_MODIFIED_TIME         NAME
    43452   Tue Nov 06 10:46:44 PST 2007    linux_session.log
     7630   Thu Nov 15 16:18:22 PST 2007    install.log
     8508   Thu Nov 15 16:18:00 PST 2007    dmesg
        0   Thu Nov 01 18:12:34 PDT 2007    eem.log
  4614755   Thu Nov 15 16:16:50 PST 2007    messages.log.prev
```

Related Commands

Command	Description
log level	Configures the severity of messages to be logged.
log trace	Configures trace logging options.

show memory

To display memory statistics, use the **show memory** command in Cisco AXP EXEC mode.

show memory [|]

Syntax Description

|	(Optional) Pipe output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, the **show memory** command displays the memory statistics.

```
se-Module> show memory
SDRAM (MByte):                512
Total Memory (kB):            512788
Active Memory (kB):           129232
Inactive Memory (kB):         105632
Other Memory (kB):            21472
MemoryPool (kB):              256452

Kernel Memory
MAXUSED(S) INUSE(S) INUSE(O) MAXUSED(O)     ERR TYPE
      4976     4904     4535       4680       0 fs
     12992    12424    11549      12322       0 other
       128      124       98        110       0 net
S - Slab memory
O - Object memory
```

Related Commands

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

show netconf session

To display Network Configuration Protocol (NETCONF) sessions, use the **show netconf session** command in Cisco AXP EXEC mode.

show netconf session [|]

Syntax Description

|	(Optional) Pipe output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

This command displays the NETCONF session configured on the router and the Cisco AXP service module.

This command displays open connections in large networks of intermittently connected devices and those devices that must reverse the management connection where firewalls and network address translators (NATs) exist.

Examples

In the following example, because there are no open sessions, the **show netconf sessions** command displays a *no open corrections* replay.

```
se-Module> show netconf session
% No open connections
```

Related Commands

Command	Description
netconf	Configures the network configuration management system (NETCONF).

show ntp associations

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

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

Syntax Description

assoc-ID *association-id*	(Optional) Specified association ID.
|	(Optional) Pipe output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

The **show ntp associations** command displays the association identifier and status for all the NTP servers configured for Cisco AXP and does not provide 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 2.
- The second two digits indicate the number of events and the type of the last event. See Table 2.

Table 2 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 2 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, is reachable, and uses proper authentication.
8xxx	Server is configured and not authenticated or reachable.
9xxx	Server is configured and reachable.
Cxxx	Server is configured to use authentication but is not reachable.

Table 2 Status Field Code Descriptions (continued)

Status Field Codes	Description
Dxxx	Server is configured to use authentication and is reachable but is not using a trusted key.
Fxxx	Server is authenticated as a trusted server and is reachable.
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 too far away also.
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 3 lists the event codes. The third digit indicates the number of events that have 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 3 Event Field Code Values

Event Field Codes	Description
xxx0	Unspecified event. Either no events have occurred or some sort of 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 3 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 4 lists the flash bits for each test.

Table 4 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.
0x200	TEST10. Autokey protocol has detected an authentication failure.

Table 4 Flash Field Diagnostic Bit Values (continued)

Flash Bit Values	Description
0x400	TEST11. Autokey protocol has not verified 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-Module> show ntp associations

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

Table 5 describes the significant fields shown in the display.

Table 5 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 1 and Table 2 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: • ok • bad • none • “ ”

Table 5 show ntp associations Field Descriptions (continued)

Field	Description
condition	Type of association in the clock selection process. Valid values are: • space: Reject. Peer is discarded as unreachable. • falsetick: 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: • (empty) • IP error • Auth fail • lost reach • reachable • clock expt See Table 2 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 should be 1 or 0.

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

```
se-Module> 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 6 describes the significant fields shown in the display.

Table 6 show ntp associations assoc-id Field Descriptions

Field	Description
status	Status of the peer. See Table 1, Table 2, and Table 4 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: • 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: • 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.
hmode	Association mode of the host server. Valid values are: • 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

Table 6 show ntp associations assoc-id Field Descriptions (continued)

Field	Description
pmode	Association mode of the peer server. Valid values are: • 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 4.
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 have been from a specific time server.
jitter	Estimated time error, in milliseconds, of the Cisco AXP 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 has never been synchronized, the value is zero.
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 the sender.
filtdelay	Round-trip delay, in seconds, between the peer clock and the local clock over the network between them.

Table 6 show ntp associations assoc-id Field Descriptions (continued)

Field	Description
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 config

To display a list of Network Time Protocol (NTP) server configurations, use the **show ntp config** command in Cisco AXP EXEC mode.

show ntp config [|]

Syntax Description

|	(Optional) Pipe output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use the **show ntp config** command after changing the ntp server configuration.

Examples

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

```
se-Module> show ntp config
NTP server 1:                1.2.3.4

NTP server 2:                1.100.30.150
```

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 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 Cisco AXP EXEC mode.

show ntp servers [|]

Syntax Description

|	(Optional) Pipe output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP 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-Module> 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,          - outlyer
+ candidate,        # selected,        * sys.peer,        o pps.peer
```

Table 7 describes the significant fields shown in the display.

Table 7 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.

Table 7 show ntp servers Field Descriptions (continued)

Field	Description
t	Type of peer. Valid values are: • l: Local • u: Unicast • m: Multicast • b: Broadcast
when	Time when the last packet was received.
poll	Polling interval, in seconds.
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 AXP clock measured as an exponential average of RMS time differences.
(tally code)	The character preceding the remote IP address indicates the status of the association in the clock selection process. Valid values are: • 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 Cisco AXP EXEC mode. The display extends back to the primary time source, starting from the localhost.

show ntp source [**detail** | |]

Syntax Description

detail	(Optional) Additional NTP server details including: precision, leap, refid, delay, dispersion, rootdelay, rootdispersion, reference time, originate timestamp, and transmit timestamp.
|	(Optional) Pipe output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

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

```
se-Module> 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 8 describes the significant fields shown in the display.

Table 8 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: • 0: Unspecified • 1: Primary clock reference • 2–255: Secondary reference by NTP
offset	Time offset between the host and the local host, in seconds.
synch distance	Host synchronization distance, which is the estimated error from the primary source.

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

```
se-Module> 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 9 describes the significant fields shown in the display.

Table 9 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: • 0: Unspecified • 1: Primary clock reference • 2–255: Secondary reference by the 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: • 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 specific 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.

Table 9 show ntp source detail Field Descriptions (continued)

Field	Description
synch dist	Host synchronization distance, which is the estimated error from the primary source.
reference time	Local time, in time-stamp format, when the local clock was last updated. If the local clock has never been 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 status 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 Cisco AXP EXEC mode.

show ntp status [|]

Syntax Description

|	(Optional) Pipe output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

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

```
se-Module> 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 10 describes the significant fields shown in the display.

Table 10 show ntp status Field Descriptions

Field	Description
NTP reference server 1	IP address of the NTP server.
Status	Status of the peer association in the clock selection process. Valid values are: • 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.
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 AXP 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 Cisco AXP.
show clock detail	Displays clock statistics.

show packets

To display packet traffic statistics, use the **show packets** command in Cisco AXP EXEC mode.

show packets [**retrieve** | **store** | |]

Syntax Description

retrieve	(Optional) Displays the packet traffic log.
store	(Optional) Saves packets until the packet traffic log is full.
|	(Optional) Pipe output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

Displaying the **show packets** command options causes a stream of output to the console. Use the Ctrl-C keys to stop the output.

Examples

The following shows sample output for the **show packets** command. To prevent data flooding the console, use the **Ctrl-C** keys to stop the output.

```
se-Module> show packets
Press control-C to exit...
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 68 bytes
15:38:18.775051 00:1e:7a:e1:41:b8 > 00:0e:0c:6f:0f:e6 sap aa ui/C
15:38:18.818643 00:0e:0c:6f:0f:e6 > 00:1e:7a:e1:41:b8 sap aa ui/C
15:38:31.982519 00:1e:7a:e1:41:b8 > ab:00:00:02:00:00, ethertype MOP RC (0x6002
), length 77:
        0x0000:  3d00 0700 0000 0100 0303 0000 0200 0221  =..............!
        0x0010:  0003 0006 0000 0000 0000 0400 023c 0005  .............<..
        0x0020:  0002 d805 0600 0200 0107 0006 001e 7ae1  ..............z.
        0x0030:  41b8 6400 0179                           A.d..y
15:38:41.130172 CDPv2, ttl: 180s, Device-ID 'axp-docs'[|cdp]
15:38:48.773615 00:1e:7a:e1:41:b8 > 00:0e:0c:6f:0f:e6 sap aa ui/C
15:38:48.773646 00:0e:0c:6f:0f:e6 > 00:1e:7a:e1:41:b8 sap aa ui/C
-- More --
```

Related Commands

Command	Description
show log name	Displays recent system event messages.

show parser

To display parser information, use the **show parser** command in Cisco AXP EXEC mode.

show parser {**commands** | **help**}

Syntax Description

commands	Displays all the CLI commands.
help	Displays the help text of each command.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

Displaying the **show parser** command options causes a stream of output to the console. Use the Ctrl-C keys to stop the output.

show process

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

show process [**all** | **memory** | **pid** *id* | **running**}

Syntax Description

all	Displays a snapshot of all processes and summary information.
memory	Displays random access memory utilization.
pid *id*	Displays a snapshot of the process, where *id* is the process identifier.
running	Displays a snapshot of the current running processes.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP application service EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

This command displays all processes in the virtual application environment and sorted by process ID in ascending order.

Examples

In the following example, **show process** displays summary and process information on the screen.

```
se-Module(exec-mping)> show process
USER PID %CPU %MEM    VSZ   RSS TTY STAT START   TIME COMMAND
root 1    0.0  0.1   1972   612 ?    S   Nov05   0:00 init [4]
root 8522 0.0  0.1   2244   800 ?    Ss  Nov05   0:00 /cisco/bin/syslog_ng
root 8523 0.0  0.1   1952   536 ?    Ss  Nov05   0:00 /bin/logmgr/var/log/messages.log
5000000
```

Related Commands

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

show processes

To display processes running on the Cisco AXP service module, use the **show processes** command in Cisco AXP EXEC mode.

show processes [**cpu** | **memory** | |]

Syntax Description

cpu	(Optional) Central processing unit utilization.
memory	(Optional) Random access memory utilization.
|	(Optional) Pipe output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, **show processes** displays all the running processes. For each process the name of the process (in the CMD column), the health of the process, and the state of the process are displayed on the screen.

```
se-Module(exec-mping)> show processes
se-Module> show processes
STATE                    HEALTH   CMD
online                   alive    syslog-ng
online                   alive    platform_config
online                   alive    trace
online                   alive    rbcp
online                   alive    ntp
online                   alive    downloader
online                   alive    superthread
online                   alive    dns
online                   alive    backuprestore
online                   alive    cli
service                  alive    sshd
```

In the following example, **show processes memory** displays the Random Access Memory (RAM) utilization of the ten running processes on the screen.

```
se-Module> show processes memory
   VSZ   RSS   SHR   PVT    RD    RW   EXE   DAT   STK  %PVT CMD
 12680  1360   968   392     0     0    96  4800     0   0.1 syslog-ng
 22704  1336  1076   260     0     0    64 14840     0   0.1 platform_config
 10384  1072   900   172     0     0    28  2552     0   0.0 rbcp
 14272  2568  1260  1308     0     0    16  4620     0   0.3 trace
  2560   772   568   204     0     0   572   464     0   0.0 monitor
 23504  3808  1456  2352     0     0    20 13848     0   0.5 downloader
 18832  1364  1120   244     0     0   212 10812     0   0.0 ntp
 63660 17780  2324 15456     0     0    40 53424     0   3.0 superthread
 63660 17780  2324 15456     0     0    40 53424     0   3.0 cli
  1972   616   524    92     0     0    28   496     0   0.0 sshd

-----------------------------------------
Process Memory Information for helloworld
-----------------------------------------
VSZ     RSS     SHR     PVT     RD      RW      EXE     DAT     STK     CMD
1972    616     524     92      0       0       28      496     0       init
2244    872     704     168     0       0       92      572     0       syslog_ng
2500    1096    948     148     0       0       572     404     0       hello_world.sh
1948    532     456     76      0       0       8       492     0       logmgr
0       0       0       0       0       0       0       0       0
```

In the following example, **show processes cpu** displays the CPU utilization of the the combined running processes on the screen.

```
se-Module> show processes cpu
Uptime (secs):                1122639.02
User time (secs):             9834.87
Kernel time (secs):           11647.49
Idle time (secs):             1100952.01
se-Module>
```

Related Commands

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

show resource limits

To display the system resource limits set for the host OS and each installed application, use the **show resource limits** command in Cisco AXP EXEC mode.

To display a summary of the resource limits configuration for the virtual application environment, use the **show resource limits** command in Cisco AXP application service EXEC mode.

show resource limits [**cpu** | **disk** | **memory**]

show resource limits

Syntax Description

cpu	(Optional) Displays detailed CPU resource limits
disk	(Optional) Displays detailed disk resource limits
memory	(Optional) Displays detailed memory resource limits

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC

Cisco AXP application service EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.
1.1	**memory**, **disk** and **cpu** keywords were introduced.

Usage Guidelines

The usage guidelines consist of the following sections:

- Resource Limits in Cisco AXP EXEC Mode (Flexible Resource Allocation)
- Resource Limits in Cisco AXP Application Service EXEC Mode

Resource Limits in Cisco AXP EXEC mode (Flexible Resource Allocation):

For resource limits that are not currently effective after the last change, the show resource limits command appends an * after each limit value, to indicate that the new values are in a pending state.

If you do not execute the **write memory** or the **copy running-config startup-config** command**,** the CLI configured value is lost after a reboot.

Table 11 shows example output values from the command **show resource limits**.

Values with ***** indicate that the user has not yet executed **write memory** and **reload**.

Table 11 show resource limits Cisco AXP EXEC Mode Command Output

Application	CPU (Index)	Memory (MB)	Disk (MB)	Log (MB)
LinuxPackage	100	100*	10*	5
TestPackage	200*	400	20	5
System Total	500	550	210	-
Resources available	480	10	78200	-

Resource Limits in Cisco AXP Application Service EXEC Mode:

Use the **show resource limits** command in Cisco AXP application service EXEC mode to view resource limits described in Table 12.

Table 12 show resource limits: Application/Application Name

Application	Application Name	Description
Cpu Package	Value for CPU requirement in Index	Resource limit generated by the packaging tool, specified during packaging.
Mem Package	Value for Mem requirement in MB	Resource limit generated by the packaging tool, specified during packaging.
Disk Package	Value for Disk requirement in MB	Resource limit generated by the packaging tool, specified during packaging.
Cpu Configured	Value for CLI Configured CPU	Resource limit configured through CLI config commands. If no limit is configured through CLI, a dash “-” is displayed.
Mem Configured	Value for CLI Configured Mem	Resource limit configured through CLI config commands. If no limit is configured through CLI, a dash “-” is displayed.
Disk Configured	Value for CLI Configured disk	Resource limit configured through CLI config commands. If no limit is configured through CLI, a dash “-” is displayed.
Cpu Limit	Value for actual CPU limit	Resource limit currently used by the system and vservers. The value may change if resources are rebalanced.
Mem Limit	Value for actual Mem limit	Resource limit currently used by the system and vservers. The value may change if resources are rebalanced.
Disk Limit	Value for actual Disk limit	Resource limit currently used by the system and vservers. The value may change if resources are rebalanced.

Examples

In the following example, **show resource limits memory** in Cisco AXP EXEC mode shows detailed memory limits for the application.

```
se-Module> show resource limits memory
APPLICATION                 app1
Packaged Memory Limit       10 MB
Configured Memory Limit      -
Current Memory Limit        464 MB
Memory Wildcard             True
```

Related Commands

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

show running-config

To display the current running configuration of the module, use the **show running-config** command in Cisco AXP EXEC mode.

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

show running-config [**paged** | |]

show running-config

Syntax Description

paged	(Optional) Displays enough output to fill the current viewing screen.
|	(Optional) Pipe output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Cisco AXP application service EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, **show running-config** displays the running configuration for the module in Cisco AXP EXEC mode.

```
se-1-100-30-50> show running-config
Generating configuration:


clock timezone America/Los_Angeles

hostname se-1-100-30-50

system language preferred "en_US"

ntp server 1.100.30.150 prefer

software download server url "ftp://127.0.0.1/ftp" credentials hidden "6u/dKTN/"
```

```
log trace local enable

no service password-encryption

interface eth0
 ip address 1.100.30.2 255.255.255.0
 exit

interface eth1
 exit

ip ssh server

app-service helloworld
 bind interface eth0
 hostname se-1-100-30-151
 exit

app-service iosapi
 hostname se-1-100-30-151
 exit

app-service showtime
 hostname se-1-100-30-151
 exit

end
```

In the next example, **show running-config** displays the running configuration for the application mping on the screen.

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

Related Commands

Command	Description
copy running-config	Copies the current system configuration to the selected destination.
show tech-support	Displays a summary of the diagnostic information for the application.

show software

To display the current software information of the module, use the **show software** command in Cisco AXP EXEC mode.

show software {**dependencies** | **directory** {**downgrade** | **download**} | **download server** | **licenses** | **packages**}

Syntax Description

dependencies	Displays the subsystem software dependencies on the installed packages.
directory	Displays the software directories.
download server	Displays information about the download server.
downgrade	Displays directory listings information about the downgrade directories.
download	Displays directory listings information about the download directories.
licenses	Displays installed software license information.
packages	Displays information about the installed software and plug-in packages.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, the **show software directory download** command shows download directory information to the screen.

```
se-Module> show software directory download

KBytes  Directory
27347   /dwnld/pkgdata

Directory listings

Directory: /dwnld/pkgdata

total 27347
drwxrwxr-x    2 root     daemon        136 Oct 18 19:30 .
drwxrwxr-x    4 root     daemon        136 Oct 18 19:30 ..
-rw-rw-r--    1 root     root     27857860 Oct 18 19:31 axp-upgrade.2.1
-rw-rw-r--    1 root     root       113161 Oct 18 19:30 axp.2.1.pkg
se-Module
```

In the next example, the **show software directory downgrade** command displays downgrade directory information to the screen.

```
se-Module> show software directory downgrade

KBytes  Directory
6154    /dwnld/dwngrade

Directory listings

Directory: /dwnld/dwngrade

total 6154
drwxrwxrwx    3 root     daemon        184 Nov  3 17:22 .
drwxrwxr-x    4 root     daemon        360 Nov  3 17:22 ..
-rw-rw-r--    1 root     daemon        227 Oct 28 18:42 .uninstall_work_order
-rw-rw-r--    1 root     daemon    6286628 Oct 28 18:42 add_files.fhdr
drwxrwxr-x    2 root     daemon         48 Nov  3 17:22 tmp
```

In the following four examples, **show software** commands display information about the installed software packages of the module.

```
se-Module> show software download server

Download server URL is: ftp://172.16.0.1/ftp

se-Module> show software licenses

Core:
 - application mode: AXP

se-Module> show software packages

Installed Packages:

 - Installer (Installer application) (1.1.0.150)
 - Bootloader (Primary) (Service Engine Bootloader) (1.0.2)
 - AXP (Virtual Server Development System) (1.1.0)
 - Infrastructure (Service Engine Infrastructure) (2.4.30.6)
 - Global (Global manifest) (1.1.0)
 - guest_os (AXP Guest OS Add-on Package) (1.1.0)
 - Bootloader (Secondary) (Service Engine Bootloader) (1.0.2.150)
 - Core (Service Engine OS Core) (2.4.30.6)
 - GPL Infrastructure (Service Engine GPL Infrastructure) (2.2.30.1)

Installed Plug-ins:

 - showtime (showtime Discus Beta) (1.3)
 - iosapi (ios api Discus app!) (1.0)
 - cli_plugin (CLI Plugin bundle to allow custom CLI plugin) (1.1.0)
 - Tomcat (Apache Foundation Tomcat Servlet Container) (5.5.20)
 - helloworld (hello Discus Beta) (1.0)

se-Module> show software versions

Installed Packages:
Software Version: 3.0.1
 - Installer  3.0.1.0
    - Thirdparty 2.3.1.0
    - Bootloader (Primary) 2.1.14
    - Infrastructure  2.3.2.0
```

Related Commands

Command	Description
software install	Installs host and add-on packages on the Cisco AXP service module

show ssh-server

To display the current status of the SSH server for a virtual instance, use the **show ssh-server** command in Cisco AXP application service EXEC mode.

show ssh-server

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP application service EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to display the status of the SSH server—either RUNNING or NOT RUNNING.

Examples

In the following example, the status of the SSH server for the virtual instance of the application SYSLOG_APP1 is displayed on the screen. In this case the SSH server is RUNNING.

```
se-Module> app-service SYSLOG_APP1
se-Module(exec-SYSLOG_APP1)> show ssh-server
Application SSH Server
Status: RUNNING
se-Module(exec-SYSLOG_APP1)>
```

Related Commands

Command	Description
ip ssh-server	Configures the SSH server.
ip ssh username	Configures SSH tunneling.

show startup-config

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

show startup-config [**paged**]

Syntax Description

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

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

This command displays the startup configuration stored in flash memory.

Examples

The following example output from the **show startup-config** command shows the stored configuration on the screen.

```
se-Module> 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.

Command	Description
show running-config	Displays the current running configuration.
write	Copies the running configuration to the startup configuration.

show state

To display the status and health of a specific application, use the **show state** command in Cisco AXP application service EXEC mode.

show state

Syntax Description

There are no arguments or keywords for this command.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP application service EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

The **show state** command displays the state and health as:

- State: Online, Offline, Pending-online, Pending-offline.
- Health: Alive, or Down.

Examples

In the following example, **show state** displays the state and health status of the application helloworld on the screen.

```
se-Module(exec-helloworld)> show state
APPLICATION STATE HEALTH
helloworld online ALIVE
```

Related Commands

Command	Description
show app-service state	Displays a list of all the installed virtual instances and applications.
show tech-support	Displays a summary of the diagnostic information for the application.

show statistics

To display statistics for a virtual instance in the application environment, use the **show statistics** command in Cisco AXP application service EXEC mode.

show statistics

Command Default

None.

Command Modes

Cisco AXP application service EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

The **show statistics** command displays statistics such as CPU utilization and memory for a virtual instance in the application environment.

The **show statistics app** command displays statistics of third party applications integrated into the application environment.

When this command is initiated, */bin/appstats* is executed. The third party application must provide the *appstats* file, in binary or script format, to plug in for its statistics.

Examples

In the following example, **show statistics** displays statistics for the environment of application "mping" on the screen.

```
se-Module(exec-mping)> show statistics
CTX PROC  VSZ   RSS   userTIME  sysTIME  UPTIME  NAME
2    3    6.6M  2.5M  0m00s12   0m00s40  3h04m08 mping

CTX = context number for the virtual instance
PROC = quantity of processes in the context
VSZ = number of pages of virtual memory
RSS = Resident set size limits for memory
userTime = utime User-mode CPU time accumulated
sysTIME = ctime Kernel-mode CPU time accumulated
UPTIME = uptime
NAME = application name
```

Related Commands

Command	Description
show statistics app	Allows third party applications to integrate their own application statistics for display.

show statistics app

To allow third party applications to integrate their own application statistics for display, use the **show statistics app** command in Cisco AXP application service EXEC mode.

show statistics app

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP application service EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

When this command is initiated, */bin/appstats* is executed which plugs in statistics that must be provided by the third party application using file *appstats* (in binary or script format).

Related Commands

Command	Description
show statistics	Displays statistics for a virtual instance in the application environment.

show status-monitor

To display parameters of the status monitor, use the **show status-monitor** command in Cisco AXP application service EXEC mode.

show status-monitor

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Cisco AXP application service EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, the **show status-monitor** command displays the status of the status-monitor for the helloworld application.

```
se-Module(exec-helloworld)> show status-monitor
Application: helloworld
Monitor status: PASSED
Monitor in progress: Yes
Last executed watchdog: W00template.sh
Last executed date: Wed Sep  5 14:09:58 PDT 2007
Last failed watchdog: ---
Last failed return code: -
Last failed date: ---
Last restarted date: ---
Recovery threshold: 4
Monitor interval: 3
```

Table 13 lists and describes the **show status-monitor** fields.

Table 13 show status-monitor Field Descriptions

Field	Description
Monitor status	IP address of the NTP server. `---` : Monitor has not been turned ON. `Passed` : Monitoring reports successful execution of watchdog scripts. `Recover` : Monitoring reports a watchdog failure, or the watchdog is taking longer than the monitor interval to return a value. The virtual instance restarts if the recovery threshold period is exceeded.

Related Commands

Command	Description
show app-service state	Displays a list of all the installed virtual instances and applications.
show tech-support	Displays a summary of the diagnostic information for the application.

show swap usage

To view the swap usage of each application, use the **show swap usage** command in Cisco AXP EXEC mode.

show swap usage

Syntax Description

There are no arguments for this command.

Defaults

None

Command Modes

Cisco AXP EXEC

Command History

Cisco AXP Release	Modification
1.1	This command was introduced.

Usage Guidelines

This command is available inside each application's context. The **show tech-support** command also displays swap usage information.

Related Commands

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

show syslog-server logs

To display syslog server log files in the /var/remote log directory, use the **show syslog-server logs** command in Cisco AXP EXEC mode.

show syslog-server logs

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

This command displays all the syslog files under /var/remote log directory.

Examples

The following example illustrates the **show syslog-server logs** command that displays the size last modified date and time for each of the syslog files under the /var/remote log directory. In this case, there is only one syslog file: remote_messages.log.

```
se-Module> show syslog-server logs
SIZE   LAST_MODIFIED_TIME               NAME
62     Thu Oct 18 16:37:22 PDT 2007     remote_messages.log
```

Related Commands

Command	Description
log level	Configures the severity of messages to be logged.
log trace	Configures trace logging options.

show syslog-server log name

To display system level logging data for a specific log file, use the **show log name** command in Cisco AXP EXEC mode.

show syslog-server log name *log-name* {**paged** | |}

Syntax Description

log-name	Log name. See the **show logs** command for log names.
paged	(Optional) Displays enough output to fill the current viewing screen.
|	Pipes output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

In the following example, **show syslog-server log name** displays system level logging data for log file remote_messages.log.

```
se-Module> show syslog-server log name remote_messages.log
Press <CTRL-C> to exit...
#!/bin/cat
16:37:22 logmgr: BEGIN FILE
16:37:22 logmgr: START
```

Related Commands

Command	Description
show logs	Displays log files in the application environment or on the Cisco AXP service module.
show syslog-server logs	Displays all the syslog files.

show system language

To display which language the system is configured to use and/or a list of the languages available, use the **show system language** command in Cisco AXP EXEC mode.

show system language {preferred | installed}

Syntax Description

installed	The languages that are available for use.
preferred	The language the system is using.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to either see the current language used by the system or the languages available to be used by the system.

Examples

The following example shows that English is the system language preferred.

```
se-Module> show system language preferred
Preferred Language: en_US
```

Related Commands

Command	Description
system language preferred	Configures the system language.

show tech-support

To display diagnostic information about the application environment, use the **show tech-support** command in Cisco AXP application service EXEC mode.

show tech-support

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Cisco AXP application service EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

This command:

- Dumps information to the screen provided by the third party application
- Displays the running-config, state, resource limits, and statistics about the application environment
- Executes the **/bin/techsupport** binary or script file to display application specific information if provided by the third-party application.
- Displays kernel capabilities
- Displays details on Linux Kernel Module(LKM) support

Examples

In the following example, **show tech-support** displays diagnostic information for the application environment on the screen. This information includes: state, statistics, processes, resource limits, and running configuration.

```
se-Module(exec-demo)> show tech-support

------------------ show app-service state ------------------
                   APPLICATION               STATE               HEALTH
                    helloworld              online                ALIVE

------------------ show app-service statistics ------------------
CTX   PROC    VSZ    RSS  userTIME   sysTIME    UPTIME NAME
0      122   2.7G 624.3M  59m23s94   1h10m58   4d20h45 root server
2        4   8.6M   2.9M   1m16s66   1m31s31   4d20h43 helloworld


------------------ show process ------------------
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.1   1972   616 ?        S    Nov15   0:00 init [4]
root      3758  0.0  0.1   2244   872 ?        Ss   Nov15   0:00 /usr/bin/syslog_ng
```

```
root      3763  0.0  0.2   2500  1096 ?        S    Nov15   0:00 /bin/bash
/opt/helloworld/hello_world.sh
root     29302  0.0  0.1   1948   532 ?        Ss   12:55   0:00 /bin/logmgr
/var/log/messages.log 5000000
root     31016  0.0  0.1   2216   532 ?        S    13:02   0:00 sleep 5


-------------------- Swap space Information --------------------

swap is turned ON

Filename  Type      Size     Used   Priority
/dev/sda3 partition 1959920  0     -2


------------------ show resource limits ------------------
    APPLICATION      CPU(INDEX)      MEMORY(MB)   DISK(MB)    LOG(MB)
     helloworld             800              10         20          5

------------------ Application Capabilities------------------
System Capabilities:
                DAC_OVERRIDE
                DAC_READ_SEARCH
                FOWNER
                FSETID
                KILL
                SETGID
                SETUID
                SETPCAP
                NET_ADMIN
Context Capabilities:
                UTSNAME
                RLIMIT
                RAW_ICMP
                SYSLOG
                SECURE_MOUNT
                SECURE_REMOUNT
                BINARY_MOUNT
                QUOTA_CTL
Dev FS:
                /dev/null c 1 4
                /dev/mytest b 20 8
                /dev/loop0 b 7 0
                /dev/loop1 b 7 1
Net Flags:
Proc FS:
                /proc/test blah
                /proc/sys/net/ipv4/ip_forward 0
Kernel Modules:
                cisco_module.ko
                /mymod/capture.ko

The following capabilities have errors when applied:
Proc FS:  /proc/test blah
Kernel Modules:  cisco_module.ko

The following capabilities have errors during installation:
System Capabilities: SYS_ADMIN

------------------ show running-config ------------------
Generating running configuration:

app-service helloworld
 bind interface eth0
```

```
hostname se-10-0-0-0
log level info
exit
```

Related Commands

Command	Description
show resource limits	Displays a summary of the resource limits configuration.
show running-config	Displays the running configuration of the application environment.
show state	Displays the status and health of a specific application.
show statistics	Displays statistics for a virtual instance in the application environment.

show trace buffer

To display a list of events in memory, use the **show trace buffer** command in Cisco AXP EXEC mode.

show trace buffer [**containing** *string* [**long** [**paged** | |] | **short** [**paged** | |]] | **long** [**paged** | |] | **short** [**paged** | |] | **tail** [*number* [**long** [**paged** | |] | **short** [**paged** | |] | [|]]]

Syntax Description

containing *string*	(Optional) Displays only events that match a search expression (sting within quotation marks).
long	(Optional) Displays expanded text for many error and return codes.
short	(Optional) Displays hexadecimal codes.
paged	(Optional) Displays enough output to fill the current viewing screen.
tail	(Optional) Display the latest events as they occur.
number	(Optional) Displays the most recent *number* of events.
|	(Optional) Pipe output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to monitor trace events set for debugging. Stop the output by pressing Ctrl-C.

Examples

The following example shows partial output from the **show trace buffer** command:

```
se-Module> show trace buffer

Press <CTRL-C> to exit...
238 09/19 23:23:11.041 TRAC TIMZ 0 UTC UTC 0
238 09/19 23:23:11.043 TRAC TIMZ 0 UTC UTC 0
800 09/19 23:28:04.152 WFSP MISC 0 WFSysdbLimits::WFSysdbLimits hwModuleType=NM
800 09/19 23:28:04.171 WFSP MISC 0 WFSysdbProp::getProp
800 09/19 23:28:04.171 WFSP MISC 0 keyName = limitsDir
str = /sw/apps/wf/ccnapps/limits
800 09/19 23:28:04.197 WFSP MISC 0 WFSysdbProp::getNodeXml
800 09/19 23:28:04.197 WFSP MISC 0 WFSysdbProp::getProp
800 09/19 23:28:04.198 WFSP MISC 0 keyName = limits
str = <?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?> <attrList> <a
ttrDecl purpose="CONFIG" type="INT32" maxsize="4"> <node>limits</node> <attr>max
_scripts</attr> <desc>maximum number of scripts</desc> <value>0</value> </attrDe
cl> <attrDecl purpose="CONFIG" type="INT32" maxsize="4"> <node>limits</node> <at
```

```
tr>max_prompts</attr> <desc>maximum number of prompts</desc> <value>0</value> </
attrDecl> </attrList>
800 09/19 23:28:04.199 WFSP MISC 0 WFSysdbProp::getNodeXml(str, str)
800 09/19 23:28:04.200 WFSP MISC 0 WFSysdbProp::getProp
800 09/19 23:28:04.200 WFSP MISC 0 keyName = app
```

Related Commands

Command	Description
show logs	Displays a list of the log files.

show trace store

To display a list of events from the atrace.log file, use the **show trace store** command in Cisco AXP EXEC mode.

show trace store [**containing** *string* [**long** [**paged** | |] | **short** [**paged** | |]] | **long** [**paged** | |] | **short** [**paged** | |] | **tail** [*number* [**long** [**paged** | |] | **short** [**paged** | |] | [|]]]

Syntax Description

containing *string*	(Optional) Displays only events that match a search expression.
long	(Optional) Displays expanded text for many error and return codes.
short	(Optional) Displays hexadecimal codes.
paged	(Optional) Displays enough output to fill the current viewing screen.
tail	(Optional) Display events as they occur.
number	(Optional) Displays the most recent *number* of events.
|	(Optional) Pipe output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to monitor trace events set for debugging.

Examples

The following example shows partial output from the **show trace store** command:

```
se-Module> show trace store
Press <CTRL-C> to exit...
238 09/19 23:23:11.043 TRAC TIMZ 0 UTC UTC 0
800 09/19 23:28:04.152 WFSP MISC 0 WFSysdbLimits::WFSysdbLimits hwModuleType=NM
800 09/19 23:28:04.171 WFSP MISC 0 WFSysdbProp::getProp
800 09/19 23:28:04.171 WFSP MISC 0 keyName = limitsDir
str = /sw/apps/wf/ccnapps/limits
800 09/19 23:28:04.197 WFSP MISC 0 WFSysdbProp::getNodeXml
800 09/19 23:28:04.197 WFSP MISC 0 WFSysdbProp::getProp
800 09/19 23:28:04.198 WFSP MISC 0 keyName = limits
str = <?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?> <attrList> <a
ttrDecl purpose="CONFIG" type="INT32" maxsize="4"> <node>limits</node> <attr>max
_scripts</attr> <desc>maximum number of scripts</desc> <value>0</value> </attrDe
cl> <attrDecl purpose="CONFIG" type="INT32" maxsize="4"> <node>limits</node> <at
tr>max_prompts</attr> <desc>maximum number of prompts</desc> <value>0</value> </
attrDecl> </attrList>
```

```
800 09/19 23:28:04.199 WFSP MISC 0 WFSysdbProp::getNodeXml(str, str)
800 09/19 23:28:04.200 WFSP MISC 0 WFSysdbProp::getProp
800 09/19 23:28:04.200 WFSP MISC 0 keyName = app
```

Related Commands

Command	Description
show logs	Displays a list of the log files.

show trace store-prev

To display a list of events from the atrace.log.prev file, use the **show trace store-prev** command in Cisco AXP EXEC mode.

show trace store-prev [**containing** *string* [**long** [**paged** | |] | **short** [**paged** | |]] | **long** [**paged** | |] | **short** [**paged** | |] | **tail** [*number* [**long** [**paged** | |] | **short** [**paged** | |] | [|]]]

Syntax Description

containing *string*	(Optional) Display only events that match a search expression.
long	(Optional) Displays expanded text for many error and return codes.
short	(Optional) Displays hexadecimal codes.
paged	(Optional) Displays enough output to fill the current viewing screen.
tail	(Optional) Display the latest events as they occur.
number	(Optional) Displays the most recent *number* of events.
|	(Optional) Pipe output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to monitor trace events set for debugging.

Examples

The following example shows partial output from the **show trace store-prev** command:

```
se-Module> show trace store-prev

Press <CTRL-C> to exit...
238 09/19 23:23:11.041 TRAC TIMZ 0 UTC UTC 0
238 09/19 23:23:11.043 TRAC TIMZ 0 UTC UTC 0
800 09/19 23:28:04.152 WFSP MISC 0 WFSysdbLimits::WFSysdbLimits hwModuleType=NM
800 09/19 23:28:04.171 WFSP MISC 0 WFSysdbProp::getProp
800 09/19 23:28:04.171 WFSP MISC 0 keyName = limitsDir
str = /sw/apps/wf/ccnapps/limits
800 09/19 23:28:04.197 WFSP MISC 0 WFSysdbProp::getNodeXml
800 09/19 23:28:04.197 WFSP MISC 0 WFSysdbProp::getProp
800 09/19 23:28:04.198 WFSP MISC 0 keyName = limits
str = <?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?> <attrList> <a
ttrDecl purpose="CONFIG" type="INT32" maxsize="4"> <node>limits</node> <attr>max
_scripts</attr> <desc>maximum number of scripts</desc> <value>0</value> </attrDe
cl> <attrDecl purpose="CONFIG" type="INT32" maxsize="4"> <node>limits</node> <at
```

```
tr>max_prompts</attr> <desc>maximum number of prompts</desc> <value>0</value> </
attrDecl> </attrList>
800 09/19 23:28:04.199 WFSP MISC 0 WFSysdbProp::getNodeXml(str, str)
800 09/19 23:28:04.200 WFSP MISC 0 WFSysdbProp::getProp
800 09/19 23:28:04.200 WFSP MISC 0 keyName = app
```

Related Commands

Command	Description
show logs	Displays a list of the log files.
show trace store	Displays a list of events from the atrace.log file.

show version

To display versions of Cisco AXP components, use the **show version** command in Cisco AXP EXEC mode.

show version [**|** | **begin** | **exclude** | **include** | **page**]

Syntax Description

|	(Optional) Pipe output to another command.
begin	(Optional) Display begins with the line that matches.
exclude	(Optional) Display excludes lines that match.
include	(Optional) Display includes lines that match.
page	(Optional) Displays paginated output (--More--).

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

This command displays a list of the installed Cisco AXP hardware components with their versions and serial numbers.

Examples

The following example shows the displayed details from the **show version** command, containing Cisco AXP network module details.

```
se-Module> show version
se-Module 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-302-K9
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 AXP service module CPU.
CPU Speed (MHz)	CPU speed, in MHz.
CPU Cache (KByte)	Size of the CPU cache, in KB.
Chassis Type	Type of chassis of the Cisco AXP service module.
Chassis Serial	Serial number of the chassis.
Module Type	A Cisco Network Module (NM), or a Cisco Advanced Integration Module (AIM).
Module Serial	Serial number of the Cisco AXP service module.
SATA Drive	Hard Drive on the Cisco AXP service module.
SKU	Unique ordering identifier for a Cisco AXP module.

Related Commands

Command	Description
show software	Displays the version numbers of the installed Cisco AXP software components.

software download abort

To abort a download that is in progress, use the **software download abort** command in Cisco AXP EXEC mode.

software download abort

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

The following is an example of downloading a software package to install later where the FTP server information is included on the command line.

```
se-Module> software download abort
Download request aborted.
```

Related Commands

Command	Description
software download clean	Downloads a complete package to install later.
software download status	Reports the status of a download in progress.
software download upgrade	Downloads an upgrade package to install later.

software download clean

To download software packages for installing later, use the **software download clean** command in Cisco AXP EXEC mode.

software download clean {*package-file-name* | url ftp://*ftp-server-ip-address*/*package-file-name*}

Syntax Description

package-file-name	Name of the package file for the new software.
url ftp://*ftp-server-ip-address*	URL of the FTP server.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

The following is an example of downloading a software package to install later where the FTP server information has been set in the configuration.

```
se-Module> software download clean axp-abc.2.0.1.pkg
```

The following is an example of downloading a software package to install later where the FTP server information is included on the command line.

```
se-Module> software download clean url ftp://10.16.0.2/axp-abc.2.0.1.pkg

WARNING:: This command will download the necessary software to
WARNING:: complete a clean install.  It is recommended that a backup be done
WARNING:: before installing software.

Would you like to continue? [n] y

Downloading  axp-abc.2.0.1.pkg
Bytes downloaded :  63648

Validating package signature ... done


> x
[17488 refs]
se-Module>
```

The following is an example of using the **software download status** command to check on the download progress.

```
se-Module> software download status

Download request in progress.
downloading file : axp-abc.2.0.prt1
bytes downloaded : 5536224
```

Related Commands

Command	Description
software download abort	Aborts a download that is in progress.
software download status	Reports the status of a download in progress.
software download upgrade	Downloads an upgrade package to install later.

software download secure

To configure a secure server (FTPS) software download to the Cisco AXP service module, use the **software download secure** command in Cisco AXP configuration mode.

To remove the secure server download configuration, use the **no** form of this command.

software download secure ftps://*server-ip-address*[*/dir*] [**all** [**ssltls**] | **control** [**ssltls**] | **try** [**ssltls**] [**auto** | **ssl** | **tls**] [**sslsec**][**both** | **host** | **none** | **peer**]]

no software download secure ftps://*server-ip-address*[*/dir*] [**all** [**ssltls**] | **control** [**ssltls**] | **try** [**ssltls**] [**auto** | **ssl** | **tls**] [**sslsec**][**both** | **host** | **none** | **peer**]]

Syntax Description

url ftps://*server-ip-address*	IP address of the secure FTPS server.
/dir	(Optional) The secure FTP directory on the server.
all	(Optional) Requires both control and data encryption.
ssltls	(Optional) Secure Sockets Layer (SSL)/Transport Layer Security (TLS) negotiation options.
control	(Optional) Requires only control encryption.
try	(Optional) Attempt download with secure FTPS first. If FTPS download attempt fails, try download using FTP.
auto	(Optional) Software decides the SSL/Transport Layer Security (TLS) negotiation order.
ssl	(Optional) Attempt SSL negotiation first. If SSL negotiation fails, try TLS negotiation.
tls	(Optional) Attempt TLS negotiation first. If TLS negotiation fails, try SSL negotiation.
sslsec	(Optional) SSL security configuration options.
both	(Optional) Verify both the host and the common name.
host	(Optional) Verify the common name.
none	(Optional) Verify neither the host nor common name.
peer	(Optional) Verify the host digital signature.

Command Modes

Cisco AXP configuration.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

The following is an example of setting the server information with just a root directory.

```
se-Module(config)> software download server url ftps://10.19.0.0/
```

The following is an example of setting the server information with a directory different than the root directory.

```
se-Module(config)> software download server url ftps://10.19.0.0/ftps_dir
```

The following is an example of setting the server information with a username and password.

```
se-Module(config)> software download server url ftps://10.19.0.0/ftps_dir username ftpuser
password ftppassword
```

Related Commands

Command	Description
show software	Displays the FTP server information.

software download server

To configure the FTP server address on the Cisco AXP service module, use the **software download server** command in Cisco AXP configuration mode.

To disable the software download server, use the **no** form of this command.

software download server url ftp://*server-ip-address***[/***dir***]** [**username** *username* **password** *password* | **credentials hidden** *credentials*]

no software download server url ftp://*server-ip-address***[/***dir***]**

Syntax Description

url ftp://*server-ip-address*	IP address of the FTP server.
/*dir*	(Optional) The FTP directory on the server.
username *username*	(Optional) Specifies the FTP username. If this option is not used, the default is “anonymous”.
password *password*	(Optional) Specifies the FTP password.
credentials hidden *credentials*	(Optional) Specifies the encrypted username and password value.

Command Modes

Cisco AXP configuration.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

The following is an example of setting the server information with just a root directory.

```
se-Module(config)> software download server url ftp://10.19.0.0/
```

The following is an example of setting the server information with a directory different than the root directory.

```
se-Module(config)> software download server url ftp://10.19.0.0/ftp_dir
```

The following is an example of setting the server information with a username and password.

```
se-Module(config)> software download server url ftp://10.19.0.0/ftp_dir username ftpuser
password ftppassword
```

Related Commands

Command	Description
show software	Displays the FTP server information.

software download status

To display the progress of a software download, use the **software download status** command in Cisco AXP EXEC mode.

software download status

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

The following is an example of a download in progress:

```
se-Module> software download status

Download request in progress.
downloading file : axp-abc.2.0.1.prt1
bytes downloaded : 5536224
```

The following is an example of a download that has completed:

```
se-Module> software download status

Download request completed successfully.
```

Related Commands

Command	Description
software download abort	Aborts a download that is in progress.
software download clean	Downloads a complete package to install later.
software download upgrade	Downloads an upgrade package to install later.

software download upgrade

To download software for a later upgrade, use the **software download upgrade** command in Cisco AXP EXEC mode.

software download upgrade {*package-filename* |
url ftp://*ftp-server-ip-address*[**/***dir*]**/***package-filename*} [**username** *username* **password** *password*]

Syntax Description

package-filename	Name of the package file for the new software.
url ftp://*ftp-server-ip-address*	URL of the FTP server.
/dir	(Optional) Directory other than the default.
username *username*	(Optional) Username for the FTP server.
password *password*	(Optional) Password for the FTP server.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to download files for a future upgrade.

Examples

The following is an example of downloading a software package to upgrade later where the FTP server information has been set up.

```
se-Module> software download upgrade axp-abc.2.1.pkg
```

The following is an example of downloading a software package to upgrade later where the FTP server information is included on the command line. The username and password could also be included in this command.

```
se-Module> software download upgrade url ftp://10.16.0.1/axp-abc.2.1.pkg

WARNING:: This command will download the necessary software to
WARNING:: complete an upgrade.  It is recommended that a backup be done
WARNING:: before installing software.

Would you like to continue? [n] y
url_host :10.16.0.1
url_user :null
url_uname :anonymous
url_psword :anonymous
url_proto :ftp
url_path :/
url_fname :axp-abc.2.0.0.12.pkg
url_url :ftp://10.16.0.1/

Downloading  axp-abc.2.1.pkg
```

```
Bytes downloaded :  63648

Validating package signature ... done
Validating installed manifests ..........complete.
[17497 refs]
```

Note When you download the software, there are no other prompts for subscriber input. The software package is downloaded to the service module.

The following is an example of using the **software download status** command to check on the download progress.

```
se-Module> software download status

Download request in progress.
downloading file : axp-abc.2.1.prt1
bytes downloaded : 5536224

se-Module> software download status

Download request completed successfully.
```

The following is an example of using the **show software directory download** to determine if a download has been successful:

```
se-Module> show software directory download

KBytes  Directory
0       /dwnld/pkgdata

Directory listings


Directory: /dwnld/pkgdata

total 0
drwxrwxr-x    2 root     daemon         48 Sep 15  2007 .
drwxrwxr-x    4 root     daemon        200 Sep 15  2007 ..
```

Related Commands

Command	Description
software download abort	Aborts a download that is in progress.
software download status	Reports the status of a download in progress.
show software directory	Displays directory information for software downloads and downgrades.

software install add

To install add-on packages on the Cisco AXP service module, use the **software install add** command in Cisco AXP EXEC mode.

software install add {*package-filename* | **url ftp://***ftp-server-ip-address***/***package-filename*}

Syntax Description

package-filename	Name of the add-on package file.
url ftp://*ftp-server-ip-address***/**	URL address of the FTP server where the package is located.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to install add-on packages.

For a list of software add-on packages, refer to the latest Cisco AXP release notes listed under Cisco Application eXtension Platform Modules on the Cisco AXP documentation page.

Examples

The following is an example of the command to install a new version of Cisco AXP software where the FTP server information was set in the configuration.

```
se-Module> software install add axp-eemapi.aim.1.0.5.pkg
```

The following is an example of installing a new version of Cisco AXP software where the FTP server information is included in the command line.

The system enters interactive mode, prompting you for information.

```
se-Module> software install add url ftp://10.16.0.1/ axp-eemapi.aim.1.0.5.pkg
```

Related Commands

Command	Description
software download abort	Aborts a download that is in progress.
software download status	Reports the status of a download in progress.
software download upgrade	Downloads an upgrade package to install later.
software install upgrade	Upgrades the current Cisco AXP software to a newer version.

software install clean

To install a new version of Cisco AXP software, use the **software install clean** command in Cisco AXP EXEC mode.

software install clean {*package-filename* | **url ftp://***ftp-server-ip-address*/*package-filename*}

Syntax Description

package-filename	Name of the package file for the new software.
url ftp://*ftp-server-ip-address*/	URL of the FTP server.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to download files for a new installation.

This command cleans the disk. All configuration and voice messages are lost after this step. For future upgrades and installations, verify that a backup has been done. If it has not, abort and do a backup first.

Examples

The following is an example of the command to install a new version of Cisco AXP software where the FTP server information was set in the configuration.

```
se-Module> software install clean axp-abc.2.0.pkg
```

The following is an example of installing a new version of Cisco AXP software where the FTP server information is included in the command line.

The system enters interactive mode, prompting you for information.

```
se-Module> software install clean url ftp://10.16.0.1/axp-abc.2.0.pkg
```

Related Commands

Command	Description
software download abort	Aborts a download that is in progress.
software download status	Reports the status of a download in progress.
software download upgrade	Downloads an upgrade package to install later.
software install upgrade	Upgrades the current Cisco AXP software to a newer version.

software install downgrade

The **software install downgrade** command is not supported, although it is visible upto maintenance release 1.0.6.

To downgrade Cisco AXP software to a lower release, use the same command for upgrading:

software install upgrade

software install upgrade

To upgrade to a newer version of Cisco AXP software, use the **software install upgrade** command in Cisco AXP EXEC mode.

software install upgrade {**pkg** *axp-package**.pkg*** |
url ftp://*ftp-server-ip-address/axp-package**.pkg***}

Syntax Description

pkg *axp-package**.pkg***	Specifies a package name.
url ftp://*ftp-server-ip-address/axp-package**.pkg***	Specifies the FTP server information.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to upgrade to a newer version of Cisco AXP software.

Copy the installer payload file *axp-installer-k9.<platform>.<version>.prt1* to the same FTP directory as the Cisco AXP package.

When a new release image is installed over an existing one, the old installer from the previous release is first upgraded via the package, *axp-installer-k9.<platform>.<version>.prt1*, and then the new image is installed.

Examples

The following is an example of the command to upgrade to a newer version of Cisco AXP software.

```
se-Module> software install upgrade url ftp://10.16.0.1/axp-abc.2.0.2.pkg
```

The following is an example of the command to upgrade to a newer version of Cisco AXP software if the FTP server is configured or the software files were downloaded previously with the **software download upgrade** command:

```
se-Module> software install upgrade pkg axp-abc.2.0.2.pkg
```

Related Commands

Command	Description
software download server	Configures the FTP server information.
software download upgrade	Downloads the files for a future upgrade.
software install clean	Installs a new version of the Cisco AXP software.
software install downgrade	Downgrades the current Cisco AXP software to an older version.

software remove

To remove software installed during a download or upgrade, use the **software remove** command in Cisco AXP EXEC mode.

software remove {**all** | **downgradefiles** | **downloadfiles** | **license** *filename*}

Syntax Description

all	Removes both the downgrade and the download files.
downgradefiles	Removes the downgrade files.
downloadfiles	Removes the download files.
license *filename*	Removes license of the specified license filename.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.
1.1	Command modified to add **license** keyword to remove licenses.

Examples

The following is an example of the **software remove all** command:

```
se-Module> software remove all

Download files removed
Downgrade files removed
```

The following is an example of the **software remove downgradefiles** command:

```
se-Module> software remove downgradefiles

Downgrade files removed
```

The following is an example of the **software remove downloadfiles** command:

```
se-Module> software remove downloadfiles

Download files removed
```

The following is an example of the **software remove license** command:

```
se-Module> software remove licenses

Download files removed
```

Related Commands

Command	Description
show software directory	Displays the disk usage for the download and downgrade directories.
show software licenses	Displays software licenses for installed software.

software uninstall

To uninstall software, use the **software uninstall** command in Cisco AXP EXEC mode.

software uninstall [**uid-list**]

Syntax Description

uid-list	Lists the UIDs of the currently installed software.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP Version	Modification
1.1	This command was introduced.

Examples

The following example shows the results of entering the **software uninstall** command with the **uid-list** option. You are then requested to enter **r**, **i**, **c**, or **x**, to remove, get more information, clear, or end the add-on software package.

Note None of the Add-on SSIDs are selected in the following example and none of the add-on packages are uninstalled.

```
se-Module> software uninstall

Add-On Uninstallation Menu:

 #  Selected         Add-On SSID                              Add-On Name (ver)
--------------------------------------------------------------------------------
 1             f463dc25-4749-48bd-b08c-25d8939c068b       Tomcat (5.5.20)
 2             b4b0ee92-cf8e-472b-8434-e8e7412ec71a       cli_plugin (1.1.0)
 3             1c741d0d-9eac-42b9-9b0f-caa3fd41defe       helloworld (1.0)
 4             8cec8ee5-54c3-4667-b62e-d4a31805d44a       iosapi (1.1.0)
 5             b951c689-d4cc-481c-a7fe-0971e2603815       iosapi (1.0)
 6             d1b4aef6-eb03-47a6-a537-324b76794a00       showtime (1.3)
--------------------------------------------------------------------------------

Available commands are:
r # - remove Add On for given #
i # - more information about Add On for given #
c # - clear Add On selection for given #
x - Done with Add On selection

Enter Command:x
Are you sure? [y/n]: y
There are no add-on subsystems on uninstall list.
Generating the add-on-uninstall work order :
No work order produced.
```

The next is an example of the **software uninstall uid-list** command. After the currently installed add-on software is listed, select the software add-on that you want to uninstall and enter its UID.

```
se-Module> software uninstall uid-list ?
  1c741d0d-9eac-42b9-9b0f-caa3fd41defe Add-on UID
  b4b0ee92-cf8e-472b-8434-e8e7412ec71a Add-on UID
  b951c689-d4cc-481c-a7fe-0971e2603815 Add-on UID
  d1b4aef6-eb03-47a6-a537-324b76794a00 Add-on UID
  f463dc25-4749-48bd-b08c-25d8939c068b Add-on UID
se-Module> software uninstall uid-list 1c741d0d-9eac-42b9-9b0f-caa3fd41defe Add-on UID
```

Related Commands

Command	Description
show software packages	Displays the currently installed software packages.

syslog-server

To enable the syslog server, use the **syslog-server** command in Cisco AXP configuration mode.

To disable the syslog server, use the **no** form of the command.

syslog-server

no syslog-server

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Cisco AXP configuration.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

This command enables or disables syslog server. The syslog server is disabled by default.

If the server is enabled, the Cisco AXP service module is used as a syslog server to receive all the log files from external devices.

The error message below arises if the system has less than 80G disk storage, or available disk space does not satisfy the current limits set by file size, and the number of files.

```
ERROR - system does not have enough disk space
```

This error is resolved by either unloading applications to free disk space, or by changing limits. If this error occurs, the syslog server is disabled.

Related Commands

Command	Description
syslog-server limit	Sets syslog server limits.

syslog-server limit file-rotation

To set the syslog server file rotation limits, use the **syslog-server limit file-rotation** command in Cisco AXP configuration mode.

To remove the syslog server configuration, use the **no** form of the command.

syslog-server limit file-rotation *size* [**file-size** *num*]

no syslog-server limit file-rotation *size* [**file-size** *num*]

Syntax Description

num	Defines the number of log files to be rotated. The range is 1–40 and the default is 10.
size	Defines the maximum size (in MB) of each log file. The range is 1-1000 MB and the default is 20 MB.

Command Default

None.

Command Modes

Cisco AXP configuration.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

Setting the file rotation configuration lower than the current settings causes extra log files to be deleted.

Examples

In the following example, the original current file rotation size is 5 (number of files). The **syslog-server limit file-rotation** command sets the new file rotation size to 2. This has the effect of deleting log files 3, 4, and 5.

```
syslog-server limit file-rotation 10 file-size 2
```

The message below indicates that the new file rotation value is lower than the current file rotation value.

```
WARNING – setting the new file-rotation value to 2 from the old value of 5 caused
extra log files to be removed
```

In the following example, the **syslog-server limit file-rotation** command sets the file size to 100 MB.

```
syslog-server limit file-rotation 100 file-size 2
```

The message below results from the available system disk space being insufficient for newly configured limits.

```
System does not have enough disk space.
```

In the following example, the **syslog-server limit file-rotation** command exceeds the limits for both file size and rotation. This causes the new configuration to be rejected and the original file size limit and rotation limit remain the same.

```
syslog-server limit file-rotation 1001 file-size 1001


syslog-server limit file-size 1001
                              ^
Invalid input detected at '^' marker

syslog-server limit file-rotation 20 file-size 1001
                                               ^
Invalid input detected at '^' marker.
```

Related Commands

Command	Description
syslog-server	Enables the syslog server.

syslog-server limit file-size

To set the syslog server file size limits, use the **syslog-server limit file-size** command in Cisco AXP configuration mode.

To remove the syslog server configuration, use the **no** form of the command.

syslog-server limit file-size *size* [**file-rotation** *num*]

no syslog-server limit file-size *size* [**file-rotation** *num*]

Syntax Description

num	Defines the number of log files to be rotated The range is 1–40 and the default is 10.
size	Defines the maximum size (in MB) of each log file. The range is 1-1000 MB and the default is 20 MB.

Command Default

None.

Command Modes

Cisco AXP configuration.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Usage Guidelines

syslog-server limit file-size *size* **[file-rotation** *num***]** works in a similar way to **syslog-server limit file-rotation** *num* **[file-size** *size***]**.

See the ""syslog-server limit file-rotation" section on page 197 for usage.

Examples

See the ""syslog-server limit file-rotation" section on page 197 for examples.

Related Commands

Command	Description
syslog-server	Enables the syslog server.

system language preferred

To set the preferred language on the Cisco AXP system module, use the **system language preferred** command in Cisco AXP configuration mode.

system language preferred *xx_YY*

Syntax Description

xx_YY	Set the preferred language, where *xx* represents the language code and *YY* represents the country code.

Command Default

None.

Command Modes

Cisco AXP configuration.

Command History

Cisco AXP Version	Modification
1.0	This command was introduced.

Examples

The following example sets the system preferred language to US English.

```
se-Module> config t
se-Module(config)> system language preferred en_US
se-Module(config)>
```

Related Commands

Command	Description
show running-config	Displays the content of the current running configuration.
show startup-config	Displays the content of the startup configuration.

techsupport support shell

To enter a restricted shell environment containing a limited set of diagnostic utilities used to troubleshoot the AXP system, use the **techsupport support shell** command in Cisco AXP EXEC mode.

techsupport support shell

Warning **Do not use this command without guidance from Cisco technical support. This is a restricted shell environment with a limited set of commands useful to technical support personnel for diagnosing the system. Type "help" or? to find out the list of TechSupport commands. Type "exit" or Cntrl-D to exit.**

Syntax Description

awk	Start pattern-matching utility for processing files.
cat	Send files, or standard input, to standard output.
df	Report the amount of free disk space available on mounted file systems and other file system information.
du	Display disk usage.
free	Display statistics about memory usage.
grep	Search files for lines that match a regular expression pattern or standard input for matching strings.
head	Display the first few *n* lines of a file.
iostat	Display CPU statistics and input/output statistics for devices, partitions, and network file systems.
ls	List information for the given files or content of directories.
more	List file one screenful at a time.
mpstat	Display processor-related statistics.
netstat	List network-related statistics.
pidstat	Display process-related information.
ps	Report on active processes.
sort	Sort the lines of a named text file.
tail	Display the last *n* lines of the named file.
top	Display information about the most CPU-intensive processes running.
traceroute	Display the route taken by packets to reach the specified network host
vmstat	Report virtual memory statistics.
wc	Display the number of words, new lines, and bytes in a given set of files.

Defaults

None

Command Modes Cisco AXP EXEC

Command History

Cisco AXP Release	Modification
1.1.5	This command was introduced.

Usage Guidelines In Cisco AXP EXEC mode, use this command to enter a shell that provides a set of diagnostic utilities as well as read-only access to the /var/log directory. When in the shell, type “help” to list the utilities provided by this shell. Type “exit” to exit the shell.

The **techsupport** command options viewable directories are at /var/log:

For guidance in using these command options, contact Cisco technical support.

Related Commands

Command	Description
show tech-support	Displays interfaces, memory, memory processes, running-config, software versions of installed software, disk usage, and partition information.

Examples The following example shows what is displayed when a user enters the tech-support shell.

```
se-Module> techsupport support shell
Saving session script in: techshell_session.log

This is a restricted shell environment with a limited set of commands
useful to technical support personnel for diagnosing the system.
Type "help" or ? to find out the list of TechSupport commands.
Type "exit" or Cntrl-D to exit.

techsupport>
```

The next example shows the use of help to display the list of utilities and viewable directories.

```
se-Module> techsupport support shell
Saving session script in: techshell_session.log

This is a restricted shell environment with a limited set of commands
useful to technical support personnel for diagnosing the system.
Type "help" or ? to find out the list of TechSupport commands.
Type "exit" or Cntrl-D to exit.

techsupport> help
TechSupport commands available:

awk  df  free  head    ls    mpstat   pidstat  sort  top         vmstat
cat  du  grep  iostat  more  netstat  ps       tail  traceroute  wc

TechSupport directories viewable:

/var/log

techsupport>
```

The next example shows the use of the “more” option to display messages.log.

```
techsupport> more /var/log/messages.log
08/08/10 15:56:42  system_startup:  rsrc_file:/etc/aim_rsrc_file
08/08/10 15:56:42  system_startup:  Populating resource values from /etc/aim_rsrc_file
08/08/10 15:56:43  system_startup:  rsrc_file:/etc/default_rsrc_file
08/08/10 15:56:43  system_startup:  Populating resource values from /etc/default_rsrc_file
08/08/10 15:56:44  system_startup:  rsrc_file:/etc/products/apphosting/aim_rsrc_file
--More--

For help using any of the given utilities, please type the name of the utility followed by
--help.
```

trace

To enable individual module debugging and tracing, use the **trace** command in Cisco AXP EXEC mode.

trace *module-name entity* [**activity**]

Syntax Description

module-name	Name of the Cisco AXP module used for debugging and tracing. Refer to Table 1 for module definitions.
entity	Name of the specific entity.
activity	(Optional) Name of the specific activity.

Table 15 Tracing Module Definitions

AXP_cliapi	AXP_ssh
AXP_snmp	AXP_syslogsvr
AXP_cli	AXP_cliplugin
AXP_appdebug	AXP_guestos
AXP_vserial	AXP_iosapi
AXP_eemapi	AXP_rsrcmgr
AXP_upgrade	

Defaults

None

Command Modes

Cisco AXP EXEC

Command History

Cisco AXP Release	Modification
1.0	This command was introduced.
1.1	This command was modified.

Usage Guidelines

The module names are listed in Table 1.

Related Commands

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

username ios

To create an IOS clear text, hidden, or unencrypted password for an IOS username account, use the **username ios** command in Cisco AXP configuration mode.

username ios *ios-username* **password** {**0** *clear-text-password* | **7** *hidden-password* | *unencrypted-clear-text-password*}

Syntax Description

ios-username	Username of IOS account.
password	Password for IOS account.
0	Indicates the next entry to be an insecure clear text IOS password.
clear-text-password	Insecure clear text IOS account password string.
7	Indicates the next entry to be a hidden IOS password.
hidden-password	Hidden IOS password string.
unencrypted-clear-text-password	Unencrypted IOS clear text password.

Defaults

None

Command Modes

Cisco AXP Configuration

Command History

Cisco AXP Release	Modification
1.0	This command was introduced.

Usage Guidelines

Unencrypted passwords can be re-used, the encrypted ones will have to be changed with a new one.

Examples

The following example shows setting an insecure clear text IOS password for user account jackie.

```
se-Module(config)> username ios jackie password 0 3nlais:0
```

The next example shows setting a hidden IOS password for user account jackie.

```
se-Module(config)> username ios jackie password 7
07362E590E1B1C041B1E124C0A2F2E206832752E1A01134D
```

The next example shows setting an IOS unencrypted clear text password for user account jackie.

```
se-Module(config)> username ios jackie password 3nlais:0
```

Related Commands

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

username sysadmin

To create a system adiministrator clear text, hidden, or unencrypted password for a system adminstrator username account, use the **username sysadmin** command in Cisco AXP configuration mode.

username sysadmin *sysadmin-username* **password** {**0** *clear-text-password* | **7** *hidden-password* | *unencrypted-clear-text-password*}

Syntax Description

sysadmin-username	Username of system administrator UNIX account.
password	UNIX password for the user. The password must be a minimum of 5 characters in length.
0	Indicates the next entry to be an insecure unencrypted UNIX password.
clear-text-password	Insecure unencrypted UNIX account password string.
7	Indicates the next entry to be a hidden UNIX password.
hidden-password	Hidden UNIX password string.
unencrypted-clear-text-password	Unencrypted UNIX clear text password.

Defaults

None

Command Modes

Cisco AXP Configuration

Command History

Cisco AXP Release	Modification
1.0	This command was introduced.

Usage Guidelines

Unencrypted passwords can be re-used, the encrypted ones will have to be changed with a new one.

Examples

The following example shows setting an insecure clear text UNIX password for user account jackie.

```
se-Module(config)> username ios jackie password 0 3nlais:0
```

The next example shows setting a hidden UNIX password for user account jackie.

```
se-Module(config)> username ios jackie password 7
07362E590E1B1C041B1E124C0A2F2E206832752E1A01134D
```

The next example shows setting a UNIX unencrypted clear text password for user account jackie.

```
se-Module(config)> username ios jackie password 3nlais:0
```

Related Commands

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

write

To erase, copy, or display the running configuration, use the write command in Cisco AXP EXEC mode.

write [**erase** | **memory** | **terminal**]

Syntax Description

erase	Erases the entire startup configuration with the exception of any configuration that affects the loader functionality. The startup configuration the reverts back to the factory default values. The running configuration is not affected.
memory	Writes the running configuration to the startup configuration. This is the default.
terminal	Writes the running configuration to the terminal.

Defaults

No default behavior or values.

Command Default

None.

Command Modes

Cisco AXP EXEC.

Command History

Cisco AXP 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
copy running-config startup-config	Writes the running configuration to the startup configuration.
erase startup-config	Deletes the current start up configuration.

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR

SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].