Exec Mode Commands (T-Z)

The Exec Mode is the initial entry point into the command line interface system. Exec mode commands are useful in troubleshooting and basic system monitoring.

Command Modes

This section includes the commands **telnet** through **upgrade url-blacklisting database**.

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

☞

Important The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

tcpdump kernel

Runs the tcpdump packet analyzer and prints out a description of the contents of packets on a specified network interface that match the boolean expression.

Product	All
Privilege	Security Administrator, Administrator
Command Modes	Exec

The following prompt is displayed in the Exec mode:

`[local]`*host_name*`#`

Syntax Description

tcpdump kernel *string*

string

Specifies an existing interface match string as an alaphanumeric stirng of 0 through 80 characters.

Usage Guidelines

Runs the tcpdump packet analyzer and prints out a description of the contents of packets on a specified network interface that match the boolean expression. This analyzer performs a sniff operation at the mcdma0 interface using the kernel BIA (Bump-in-the-API) as a filter. This allows sniffing of kernel traffic complete with midplane header.

☞

Important　The **tcpdump kernel** command is not available in Trusted builds.

Example

The following command initiates a tcpdump for the default kernel interface:

tcpdump BPPP

telnet

Connects to a remote host using the terminal-remote host protocol and a hostname or IPv4 address and port number.

Product	All

Privilege	Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

telnet { *host_name* **|** *host_ipv4_address* **} [port** *port_num* **]**

host_name | host_ipv4_address

Identifies the remote node with which to attempt connection.

host_name: specifies the remote node using its logical host name which must be resolved via DNS lookup.

host_ipv4_address: specifies the remote node using its assigned IP address entered using the IPv4 dotted-decimal notation.

port port_num

Specifies a specific port for connect connection as an integer from 1025 through 10000.

Usage Guidelines

Telnet to a remote node for maintenance activities and/or troubleshooting when unable to do so directly.

> ☞
>
> **Important** **telnet** is not a secure method of connecting between two hosts. **ssh** should be used whenever possible for security reasons.

Example

The following connects to remote host *remoteABC*.

telnet remoteABC

The following connects to remote host *209.165.200.229* port *2047*.

telnet 209.165.200.229 port 2047

telnet6

Connects to a remote host using the terminal-remote host protocol and a hostname or an IPv6 address and port number.

Product	All

Privilege	Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

telnet6 { *host_name* **|** *host_ipv6_address* **} [port** *port_num* **]**

host_name | host_ipv6_address

Identifies the remote node with which to attempt connection.

host_name: specifies the remote node using its logical host name which must be resolved via DNS lookup.

host_ipv6_address: specifies the remote node using its assigned IP address entered using the IPv6 colon-separated-hexadecimal notation.

port *port_num*

Specifies a specific port for connect connection as an integer from 1025 through 10000.

Usage Guidelines

Telnet to a remote node for maintenance activities and/or troubleshooting when unable to do so directly.

☞

Important **telnet6** is not a secure method of connecting between two hosts. **ssh** should be used whenever possible for security reasons.

Example

The following connects to remote host *remoteABC*.

telnet6 remoteABC

The following connects to remote host *FE80::172.30.67.89* port *2047*.

telnet6 FE80::172.30.67.89 port 2047

terminal

Sets the number of rows or columns for display output.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

[local]*host_name*#

Syntax Description

terminal { length *lines* **| width** *characters* **}**

length *lines* | width *characters*

length *lines*: sets the terminal length in number of lines (rows) of text from 5 to 4294967295 lines or the special value of 0 (zero). The value 0 sets the terminal length to infinity.

width *characters*: sets the terminal width in number of characters from 5 to 512 characters.

Usage Guidelines   Set the length to 0 (infinite) when collecting the output of a command line interface session which is part of a scripted interface.

Example

The following sets the length then width in two commands.

```
terminal length 66
terminal width 160
```

The following command sets the number of rows of the terminal to infinity.

```
terminal length 0
```

test alarm

Tests the alarm capabilities of the chassis.

Product   All

Privilege   Security Administrator, Administrator, Operator, Inspector

Command Modes   Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description   **test alarm { audible | central-office { critical | major | minor } }**

audible | central-office { critical | major | minor }

audible: Tests the internal alarm on the ASR 5500 System Status Card (SSC) for 10 seconds. The alarm status is returned to its prior state, such as if the audible alarm was enabled prior to the test, the alarm will again be enabled following the test.

central-office { critical | major | minor }: Tests the specified central office alarm type.

Usage Guidelines   Test the alarm capabilities of the chassis as periodic maintenance to verify the hardware for generation of the internal audible alarms is functional.

⚠️

Caution   The use of test commands could adversely affect the operation of your system. It is recommended that they only be used under the guidance and supervision of qualified support representative.

Example

```
test alarm audible
test alarm central-office critical
test alarm central-office major
test alarm central-office minor
```

test ggsn vapn

Tests for Virtual Access Point Names (VAPNs) in GGSN networks.

Product	GGSN
Privilege	Security Administrator, Administrator, Operator, Inspector
Command Modes	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
test ggsn vapn { msisdn range | imsi range }
```

msisdn range | imsi range

msisdn range: Tests VAPNs within a range of previously specified Mobile Subscribers Integrated Services Digital Network (MSISDN) identifiers.

imsi range: Tests VAPNs within a range of previously specified International Mobile Subscriber Identity (IMSI) numbers.

Usage Guidelines

Test for the existence of VAPNs associated with MSISDN or IMSI numbers.

⚠

Caution   The use of test commands could adversely affect the operation of your system. It is recommended that they only be used under the guidance and supervision of qualified support representative.

Example

```
test ggsn vapn msisdn range
test ggsn vapn imsi range
```

test ipcf bindmux

Tests the status of the Intelligent Policy Control Function (IPCF) BindMux Manager instance and also starts or stops the BindMux Manager instance on the chassis.

Product	IPCF
Privilege	Security Administrator, Administrator, Operator
Command Modes	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

| **Syntax Description** | `test ipcf bindmux [ start | stop ]` |

start

Starts the IPCF BindMux Manager on the chassis. If already an instance of IPCF BindMux Manager is running it prompts accordingly.

stop

Stops the IPCF BindMux Manager instance running on the chassis.

| **Usage Guidelines** | Use this command to test the status of IPCF BindMux Manager instance and also to start or stop the BindMux Manager instance on the chassis. |

⚠️

Caution   The use of test commands could adversely affect the operation of your system. It is recommended that they only be used under the guidance and supervision of qualified support representative.

Example

The following command stops the BindMux Manager instance running on the chassis:

`test ipcf bindmux stop`

test ipsec tunnel ip-pool

Tests a specified IPSec tunnel associated with an IP pool name.

Product	All
Privilege	Security Administrator, Administrator, Operator
Command Modes	Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

| **Syntax Description** | `test ipsec tunnel ip pool` *pool_name* `destination-ip` *ip_address* `}` |

pool_name destination-ip *ip_address*

ip pool *pool_name*: Specifies the name of an existing IP pool as an alphanumeric string of 1 through 32 characters.

destination-ip *ip_address*: Specifies a destination IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation

| **Usage Guidelines** | Use this command to test a specified IPSec tunnel. |

⚠️

Caution The use of test commands could adversely affect the operation of your system. It is recommended that they only be used under the guidance and supervision of qualified support representative.

Example

The following command test the IPSec tunnel associated with *pool3* with a destination IP address of *209.165.200.229* :

```
test ipsec tunnel ip pool pool3 destination-ip 209.165.200.229
```

test mobile tunnel

Tests for the existence of a specified mobile tunnel.

Product   All

Privilege   Security Administrator, Administrator, Operator

Command Modes   Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description   `test mobile tunnel { callid` *call_id* `| imsi` *imsi_value* `| ipaddr` *ip_address* `| msid` *msid_num* `| nai` *nai_value* `}`

callid *call_id*

Specifies the exact call instance ID which is to have trace data logged.as a 4-byte hexadecimal number.

imsi *imsi_value*

Specifies the International Mobile Subscriber Identity (IMSI) of the subscriber session to be monitored an integer from 1 though 15 characters.

ipaddr *ip_address*

Specifies the IP address of the subscriber session to be monitored in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

msid *msid_num*

Specifies the mobile subscriber identification number to be monitored as 7 to 16 digits of an IMSI, MIN, or RMI.

nai *nai_value*

Specifies the mobile session Network Access Identifier as an alphanumeric string of 1 through 256 characters. The NAI is the user identity submitted by the client during network access authentication.

Usage Guidelines   Use this command to test a specified mobile tunnel.

⚠️

Caution   The use of test commands could adversely affect the operation of your system. It is recommended that they only be used under the guidance and supervision of qualified support representative.

Example

The following command tests the subscriber session associated with IP address 209.165.202.128:

```
test mobile tunnel ipaddr 209.165.202.128
```

timestamps

Enables or disables the generation of a timestamp in response to each command entered. The timestamp does not appear in any logs as it is a CLI output only. This command affects the current CLI session only. Use the **timestamps** command in the Global Configuration Mode to change the behavior for all future CLI sessions.

Product   All

Privilege   Security Administrator, Administrator, Operator, Inspector

Command Modes   Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description   `[ no ] timestamps`

no

Disables generation of timestamp output for each command entered. When omitted, the output of a timestamp for each entered command is enabled.

Usage Guidelines   Enable timestamps when logging a CLI session on a remote terminal such that each command will have a line of text indicating the time when the command was entered.

Example

The following command initiates time stamping of CLI commands as they are entered for this login session:

```
timestamps
```

traceroute

Collects information on the route data will take to a specified IPv4 host.

Product	All
Privilege	Security Administrator, Administrator, Operator, Inspector
Command Modes	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

☞

Important Inspector privileges are granted for all variables except **count and port**. To initiate a traceroute count or to target a specific port for a traceroute, you must have a minimum privilege level of Operator.

Syntax Description

```
traceroute { host_name | host_ip_address } [ count packets ] [ df ] [ maxttl
max_ttl ] [ minttl min_ttl ] [ port port_num ] [ size octet_count ] [ src {
src_host_name | src_host_ip_address } ] [ timeout seconds ] [ vrf vrf_name ] [ | {
 grep grep_options | more } ]
```

host_name | host_ip_address

Identifies the remote node to trace the route to.

host_name: specifies the remote node using its logical host name which must be resolved via DNS lookup.

host_ip_address: specifies the remote node using its assigned IP address entered using the IPv4 dotted-decimal notation.

count packets

Specifies the number of UDP probe packets to send. Default: 3

df

Indicates the packets for the tracing of the route should not be fragmented. If a packet requires fragmenting, it is dropped and the result is the ICMP response "Unreachable, Needs Fragmentation" is received.

maxttl max_ttl

Specifies the maximum time to live for the route tracing packets as an integer from 1 through 255. *max_ttl* must be greater than *min_ttl* whether *min_ttl* is specified or defaulted. Default: 30

The time to live (TTL) is the number of hops through the network; it is not a measure of time.

minttl min_ttl

Specifies the minimum time to live for the route tracing packets as an integer from 1 through 255. *min_ttl* must be less than *max_ttl* whether *max_ttl* is specified or defaulted. Default: 1

The time to live (TTL) is the number of hops through the network; it is not a measure of time.

port *port_num*

Specifies a specific port for connection as an integer from 1 through 65535. Default: 33434

size *octet_count*

Specifies the number of bytes for each packet as an integer from 40 through 32768. Default: 40

src { *src_host_name* | *src_host_ip_address* }

Specifies an IP address to use in the packets as the source node. Default: originating system's IP address

src_host_name: specifies the remote node using its logical host name which must be resolved via a DNS lookup.

src_host_ip_address: specifies the remote node using its assigned IP address specified entered using IPv4 dotted-decimal notation.

timeout *seconds*

Specifies the maximum time (in seconds) to wait for a response from each route tracing packet as an integer from 2 through 100. Default: 5

vrf *vrf_name*

Specifies the name of an existing virtual routing and forwarding (VRF) context associated with this route as an alphanumeric string of 1 through 63 characters. Associates a Virtual Routing and Forwarding (VRF) context with this static ARP entry.

grep *grep_options* | more

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in this guide.

Usage Guidelines   Trace an IPv4 route when troubleshooting network problems where certain nodes are having significant packet delays or packet loss. This can also be used to identify bottlenecks in the routing of data within the network.

Example

The following command traces the route to remote host *remoteABC* and sends the output to the more command.

```
traceroute remoteABC | more
```

The following command traces the route to remote host *209.165.200.229*'s port *2047* waiting a maximum of *2* seconds for responses.

```
traceroute 209.165.200.229 port 2047 timeout 2
```

traceroute6

Collects information on the route data will take to a specified IPv6 host.

Product	All
Privilege	Security Administrator, Administrator, Operator, Inspector
Command Modes	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

☞

Important   Inspector privileges are granted for all variables except **count and port**. To initiate a traceroute count or to target a specific port for a traceroute, you must have a minimum privilege level of Operator.

Syntax Description   **traceroute6** { *host_name* | *host_ipv6_address* } [**count** *packets*] [**maxttl** *max_ttl*] [**port** *port_num*] [**size** *octet_count*] [**src** { *src_host_name* | *src_host_ipv6_address* }] [**timeout** *seconds*] [**vrf** *vrf_name*] [| { **grep** *grep_options* | **more** }]

host_name | host_ipv6_address

Identifies the remote node to trace the route to.

host_name: specifies the remote node using its logical host name which must be resolved via DNS lookup.

host_ipv6_address: specifies the remote node using its assigned IP address entered using the IPv6 colon-separated-hexadecimal notation.

count packets

Specifies the number of UDP probe packets to send. Default: 3

maxttl max_ttl

Specifies the maximum time to live for the route tracing packets as an integer from 1 through 255. *max_ttl* must be greater than *min_ttl* whether *min_ttl* is specified or defaulted. Default: 30

The time to live (TTL) is the number of hops through the network; it is not a measure of time.

port port_num

Specifies a specific port for connection as an integer from 1 through 65535. Default: 33434

size octet_count

Specifies the number of bytes for each packet as an integer from 40 through 32768. Default: 40

src { *src_host_name* | *src_host_ipv6_address* }

Specifies an IP address to use in the packets as the source node. Default: originating system's IP address

src_host_name: specifies the remote node using its logical host name which must be resolved via a DNS lookup.

src_host_ipv6_address: specifies the remote node using its assigned IP address specified entered using IIPv6 colon-separated-hexadecimal notation.

timeout *seconds*

Specifies the maximum time (in seconds) to wait for a response from each route tracing packet as an integer from 2 through 100. Default: 5

vrf *vrf_name*

Specifies the name of an existing virtual routing and forwarding (VRF) context associated with this route as an alphanumeric string of 1 through 63 characters.

grep *grep_options* | more

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in this guide.

Usage Guidelines

Trace an IPv6 route when troubleshooting network problems where certain nodes are having significant packet delays or packet loss. This can also be used to identify bottlenecks in the routing of data within the network.

Example

The following command traces the route to remote host *remoteABC* and sends the output to the more command.

```
traceroute6 remoteABC | more
```

The following command traces the route to remote host *2000:4A2B::1f3F*'s port *2047* waiting a maximum of *2* seconds for responses.

```
traceroute6 2000:4A2B::1f3F port 2047 timeout 2
```

update active-charging

Updates specified active charging option(s) for the matching sessions.

Product

ACS

PSF

NAT

TPO

Privilege	Security Administrator, Administrator, Operator, Inspector
Command Modes	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

update active-charging { override-control rulebase-config | switch-to-fw-and-nat-policy *fw_nat_policy_name* **| switch-to-rulebase** *rulebase_name* **| switch-to-tpo-policy** *tpo_policy_name* **} { all | callid** *call_id* **| fw-and-nat-policy** *fw_nat_policy_name* **| imsi** *imsi* **| ip-address** *ip_address* **| msid** *msid* **| rulebase** *rulebase_name* **| tpo-policy** *tpo_policy_name* **| username** *user_name* **} [-noconfirm] [| { grep** *grep_options* **| more }]**

override-control rulebase-config

This keyword initiates batch processing of all active calls to apply Override Control (OC) or Inheritance after any rulebase changes, charging action changes and/or addition/deletion of ruledefs for all subscribers having OC or Inheritance feature enabled. Since this is the batch processing of all active calls, the command execution will be in the background even after the CLI command returns to the CLI prompt.

☞

Important	Override Control is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. For more information on the licensing requirements, contact your Cisco account representative. For more information on the command to enable this feature, refer to *ACS Rulebase Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

☞

Important	In this release, both Inheritance and the Override Control features are supported. Note that these two features should not be enabled simultaneously. If by mistake, these two features are enabled, only Override Control is applied.

In 17 and later releases, this CLI command is used to apply the overridden or inherited values after any ruledef, charging action and rulebase changes performed through the CLI commands in the respective configuration modes. This CLI command is necessary because the configuration changes are reflected immediately on any new PDN session that gets established. However, for the existing PDN sessions established before the configuration change, explicit execution of this CLI command is necessary. This will get all the PDN sessions in system in sync with respect to the required configuration changes.

☞

Important	It is recommended that this CLI command is executed after all rulebase/charging action/ruledef changes are complete. So, this will help in one-time execution of the CLI to get all PDN sessions in sync.

Typically, this command is used whenever any rulebase, charging action or ruledef modification happens. Once this CLI command is executed, each subscriber will read the configuration and incorporate the rulebase or ruledef changes for Override Control. Until this CLI execution is complete, Inheritance or Override Control values will not be applied to the changes done in configuration for all existing calls. Charging and policy parameters configured at P-GW will apply during this period. Please follow recommended upgrade procedures to avoid this. For the upgrade procedure, contact your Cisco account representative.

In release 17, the batch processing will complete in 15 to 20 minutes depending on the call load in the system. In 18 and later releases, batch processing will complete in 1 to 3 minutes depending on the call load in the system.

If the **override-control rulebase-config** command has been issued multiple times, batch processing will be restarted and the latest rulebase/charging action/ruledef changes will be applied to all the active calls.

☞

Important   In release 17, there was no restriction on the usage of the CLI command "**update active-charging override-control rulebase-config**" on a standby chassis. In release 18 and later, this CLI command is not allowed to be executed on the standby chassis.

switch-to-fw-and-nat-policy *fw_nat_policy_name*

Specifies an existing Firewall-and-NAT policy to switch to as an alphanumeric string of 1 through 63 characters.

switch-to-rulebase *rulebase_name*

Specifies an existing rulebase to switch to as an alphanumeric string of 1 through 63 characters.

switch-to-tpo-policy *tpo_policy_name*

☞

Important   The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

all

Updates rulebase/policy for all subscribers.

callid *call_id*

Updates rulebase/policy for the Call Identification number specified as an eight-digit hexadecimal number.

fw-and-nat-policy *fw_nat_policy_name*

Updates the rulebase/policy for sessions matching an existing Firewall-and-NAT policy specified as an alphanumeric string of 1 through 63 characters.

imsi *imsi*

Updates rulebase/policy for International Mobile Subscriber Identification (IMSI) specified here.

imsi must be 3 digits of MCC (Mobile Country Code), 2 or 3 digits of MNC (Mobile Network Code), and the rest with MSIN (Mobile Subscriber Identification Number). The total should not exceed 15 digits. For example, 123-45-678910234 can be entered as 12345678910234.

ip-address *iP_address*

Updates rulebase/policy for the IP address specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

msid *msid*

Updates rulebase/policy for an MSID specified as a string of 1 through 24 characters.

rulebase *rulebase_name*

Updates rulebase/policy for sessions matching an existing rulebase specified as an alphanumeric string of 1 through 63 characters.

tpo-policy *tpo_policy_name*

☞

Important   The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

username *user_name*

Updates rulebase/policy for user specified as a an alphanumeric of characters and/or wildcard characters ('$' and '*') of 1 through 127 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the Regulating a Command's Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage Guidelines   Use this command to change specified active charging option(s) for the matching sessions.

Example

The following command changes the rulebase for sessions using the rulebase named *standard* to use the rulebase named *super*:

```
update active-charging switch-to-rulebase super rulebase standard
```

update firewall policy

This command is obsolete.

update ip access-list

When you update an IP Access list, this command forces the new version of the access list to be applied to any subscriber sessions that are currently using that list.

Product	PDSN
	GGSN
	ASN-GW
Privilege	Security Administrator, Administrator
Command Modes	Exec
	The following prompt is displayed in the Exec mode:
	`[local]host_name#`
Syntax Description	**update ipv6 access-list** *list_name* **subscribers [** *command_keyword* **] [** *filter_keywords* **] [-noconfirm] [verbose]]**

list_name

Specifies the name of an existing IP Access list that you want to apply to the subscriber as an alphanumeric string of 1 through 47 characters.

[*command_keyword*] [*filter_keywords*]

These are the same command keywords and filter keywords available for the **show subscribers** command.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

verbose

Show detailed information.

Usage Guidelines	Use this command to force existing subscriber sessions that are already using a specific IP Access list to have that IP Access list reapplied. This is useful when you edit an IP Access list and want to make sure that even existing subscriber sessions have the new changes applied.

Example

To apply the IP Access list named *ACLlist11* to all existing subscribers that are already using that IP Access list, enter the following command:

update ip access-list ACLlist11 subscribers all

update ipv6 access-list

When you update an IP Access list, this command forces the new version of the access list to be applied to any subscriber sessions that are currently using that list.

Product	PDSN
	GGSN

ASN-GW

Privilege	Security Administrator, Administrator
Command Modes	Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

update ipv6 access-list *list_name* **subscribers [** *command_keyword* **] [** *filter_keywords* **] [-noconfirm] [verbose]]**

list_name

Specifies the name of an existing IPv6 Access list that you want to apply to the subscriber as an alphanumeric string of 1 through 47 characters.

[*command_keyword*] [*filter_keywords*]

These are the same command keywords and filter keywords available for the **show subscribers** command.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

verbose

Show detailed information.

Usage Guidelines

Use this command to force existing subscriber sessions that are already using a specific IPv6 Access list to have that IPv6 Access list reapplied. This is useful when you edit an IPv6 Access list and want to make sure that even existing subscriber sessions have the new changes applied.

Example

To apply the IPv6 Access list named *ACLv6List1* to all existing subscribers that are already using that IP Access list, enter the following command:

update ipv6 access-list ACLv6List1 subscribers all

update ip-pool apn

Use this CLI command to update the VPN manager with the APN configuration changes.

Product	CUPS
Privilege	Security Administrator, Administrator
Command Modes	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description   `update ip-pool apn { all | name apn_name }`

all

Specifies to update all the configured APNs to the VPN manager.

name apn_name

Specifies to update a specific APN configuration to the VPN manager.

Usage Guidelines   This CLI command triggers the SX_ASSOCIATION_UPDATE towards the UP and transfers all the allocated IP pool chunks for the newly added IP pools.

For additional information, refer to the *Dynamic APN and IP Pool Support* chapter.

Example

The following CLI command updates a specific APN configuration, *cisco.com*, to the VPN manager:

`update ip-pool apn name cisco.com`

update local-user database

Updates the local user (administrative) database with current user information. Run this command immediately after creating, removing or editing administrative users.

> ☞
>
> **Important**   In a release 20.0 or higher Trusted build, this command is <u>not</u> available.

Product   All

Privilege   Security Administrator, Administrator

Command Modes   Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description   `update local-user database`

Usage Guidelines   Use this command to update the local-user database with current information.

Example

The following command updates the local-user database:

`update local-user database`

update module

Loads a specified plugin module from the Module Priority List with the lowest priority number. This will also copy the Module priority list onto the Version priority list. This function is associated with the patch process for accommodating dynamic software upgrades.

Product	ADC
Privilege	Security Administrator, Administrator
Command Modes	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

update module *plugin_name*

plugin_name

Specifies the name of an existing plugin module that you want to update as an alphanumeric string of 1 through 16 characters. If the named module is not known to the system, an error message is displayed.

Usage Guidelines Use this command to initiate an update of a new software plugin module. If it fails to load, the module with next highest priority will be loaded. If none of the modules are installed, the default patch which comes along with the StarOS build is automatically loaded. The specified module must have been previously unpacked/verified and configured via the **install plugin** and **plugin** commands respectively.

For additional information, refer to the *Plugin Configuration Mode Commands* chapter.

Example

The following command updates the plugin module named *p2p*:

```
update module p2p
```

update qos policy map

Updates QoS profile information based on specific subscriber policy maps.

Product	All
Privilege	Security Administrator, Administrator
Command Modes	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
update qos policy-map map_name use-granted-profile-id id1 [ id2 ] [ id3 ]
subscribers [ command_keyword ] [ filter_keywords ] [ -noconfirm ] [ verbose ]
 [ match-requested-profile-id ] [ | { grep grep_options | more } ]
```

map_name

Specifies the name of an existing policy map as an alphanumeric string of 1 through 15 characters.

use-granted-profile-id *id1* [*id2*] [*id3*]

Specifies the profile IDs to update. Up to three different profile IDs can be specified.

Each profile ID is specified as a hexadecimal value from 0x0 and 0xFFFF.

subscribers [*command_keyword*] [*filter_keywords*]

These are the same command keywords and filter keywords available for the **show subscribers** command.

[-noconfirm]

Updates matching subscribers without prompting for confirmation.

[verbose]

Displays details for the profile updates.

[match-requested-profile-id]

Sends session-updates only to profile-ids matching the profile-ids in the requested list.

grep *grep_options* | more

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in this guide.

Usage Guidelines

Use this command to update subscriber session profile IDs based on the specified criteria.

Example

The following command updates profile IDs *0x3E* and *0x4C* for all subscriber sessions and sends session-updates with the IDs:

```
update qos policy-map test use-granted-profile-id 0x3E 0x4C subscribers
all match-requested-profile-id
```

update qos tft

Updates the subscriber traffic flow template (TFT) associated with the flow ID and direction.

Product	All
Privilege	Security Administrator, Administrator
Command Modes	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
update qos tft flow-id flow-id flow-dir { forward | reverse }
use-granted-profile-id id1 [ id2 ] [ id3 ] subscribers [ command_keyword ] [
filter_keywords ] [-noconfirm ] [ verbose ] [ match-requested-profile-id ]
[ | { grep grep_options | more }
```

flow-id *flow-id*

Sends session updates only when the flow ID matches the flow-id and flow-direction. *flow-id* must be specified as an integer from 1 through 255.

flow-dir { forward | reverse }

Specifies the direction of the TFT flow.

subscribers [*command_keyword*] [*filter_keywords*]]

These are the same command keywords and filter keywords available for the **show subscribers** command.

Usage Guidelines Supports QoS updates based on subscriber TFTs.

Example

The following command update QoS for reverse flow 0, profile ID 0x0, all subscribers without prompting for confirmation:

```
update qos tft flow-id 0 flow-dir reverse use-granted-profile-id 0x0
subscribers all -noconfirm
```

update security

Updates database information for the specified Talos Security Intelligence server.

Product	All
Privilege	Security Administrator, Administrator
Command Modes	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description **update security server talos-intelligence** *server_name* **[force]**

server_name

Specifies an existing Talos Intelligence Server name to be updated. *server_name* must be specified as a case-sensitive alphanumeric string from 1 through 31 characters.

force

Deletes the existing DB files before the Talos Intelligence server is queried. When this optional keyword is used, the latest files will always be downloaded and updated even if the system already has the most recent versions.

Usage Guidelines Use this command to query the Talos Intelligence Server to determine if updated database files exist. If so, the files will be downloaded and updated.

upgrade content-filtering

Upgrades the Static Rating Database (SRDB) for Category-based Content Filtering application.

Product CF

Privilege Security Administrator, Administrator

Command Modes Exec

The following prompt is displayed in the Exec mode:

[local]*host_name*#

Syntax Description **upgrade content-filtering category { database | rater-pkg }**

upgrade content-filtering category database

Triggers the upgrade of the Category-based Content Filtering Static Rating Database (SRDB).

upgrade content-filtering category rater-pkg

Triggers manual upgrade of the Dynamic Content-Filtering Rater Package (**rater.pkg** file).

The **rater.pkg** file contains the models and feature counters that are used to return the dynamic content rating. The upgrade will trigger distribution of the **rater.pkg** to all the SRDBs.

☞

Important This command is customer specific. For more information, please contact your local sales representative.

Usage Guidelines Use this command to load the Static Rating Database (SRDB) in to memory for Category-based Content Filtering application, and/or to load the *rater.pkg* file.

If the default directory of /cf does not exist on the flash, it will create the same. It also locates the recent full database and loads it into memory. This command also clears the old and excess incremental databases.

☞

Important   This command is not supported on all platforms.

Example

The following command upgrades the SRDB for the Category-based Content Filtering application:

upgrade content-filtering category database

upgrade database

This command allows you to upgrades a specified database.

Product	All
Privilege	Security Administrator, Administrator
Command Modes	Exec
	The following prompt is displayed in the Exec mode:
	[local]*host_name*#
Syntax Description	**upgrade database uidh [all	wl-url-host-db]**

uidh all

Upgrades UIDH databases.

uidh wl-url-host-db

Upgrades URL Host databases.

Usage Guidelines	Use the following command to upgrade the UIDH whitelist URL database:

upgrade tethering-detection

Upgrades the Tethering Detection feature's database(s).

Product	ACS
Privilege	Security Administrator, Administrator
Command Modes	Exec
	The following prompt is displayed in the Exec mode:
	[local]*host_name*#

Syntax Description	`upgrade tethering-detection database { all	os-signature	tac	ua-signature } [-noconfirm]`

all

Upgrades all Tethering Detection databases—OS, TAC and UA.

os-signature

Upgrades only the OS database.

tac

Upgrades only the TAC database.

ua-signature

Upgrades only the UA database.

- noconfirm

Executes the command without any prompts and confirmation from the user.

Usage Guidelines	Use this command to upgrade the database(s) used by the Tethering Detection feature.

This command upgrades the database(s) from file(s) kept in designated path. The name of the existing source file is prefixed with the word "new-". For example for OS DB, if the existing file name is "os-db", the upgrade file name is "new-os-db".

If there is a file named "new-xxx-db", it is verified that it is a valid Tethering Detection database and then loaded it into memory. If successful, the files is renamed "xxx-db" to "xxx-db-<number>" and then renamed "new-xxx-db" to "new-xxx-db".

For example, the command **upgrade tethering-database ua-signature -noconfirm** results in loading the file by name "new-ua-db" if it is present in the designated directory. In case of a successful upgrade, the previous version of the database is stored as backup in a file named "ua-db-1". Also, the newly uploaded database file is renamed as "ua-db".

Also see the **tethering-database** command in the *ACS Configuration Mode Commands* chapter.

Example

The following command upgrades all Tethering Detection databases:

`upgrade tethering-detection database all -noconfirm`

upgrade url-blockedlisting database

Upgrades the URL blockedlisting database.

Product	CF

Privilege	Security Administrator, Administrator

Command Modes	Exec
	The following prompt is displayed in the Exec mode:
	[local]*host_name*#
Syntax Description	In releases prior to StarOS 21.26:

upgrade url-blacklisting database [-noconfirm]

From StarOS 21.26 and later releases:

upgrade url-blockedlisting database [-noconfirm]

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines	Use this command to upgrade and load a URL blacklisting database whenever required.

Example

In releases prior to StarOS 21.26:

The following command updates the URL blacklisting database:

upgrade url-blacklisting database

From StarOS 21.26 and later releases:

The following command updates the URL blockedlisting database:

upgrade url-blockedlisting database