Exec Mode show Commands (A-C)

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

Command Modes

This section includes the commands **show aaa** through **show css service**.

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).

show active-charging analyzer statistics

Displays statistical information for protocol analyzers.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show active-charging analyzer statistics [name *protocol_name* **[instance** *instance_number* **] [verbose]] [| { grep** *grep_options* **| more }]**

name *protocol_name*

Displays detailed information for the specified protocol analyzer:

- **cdp**
- **dns**

- **file-transfer**
- **ftp**
- **h323**
- **http**
- **icmp**
- **icmpv6**
- **imap**
- **ip**
- **ipv6**
- **mms**
- **p2p [application** *p2p_list* **| protocol-group** *group_list* **| duration [audio { application** *p2p_audio_duration_list* **} | video { application** *p2p_video_duration_list* **}]] [wide [all]]** : Peer-to-peer analyzer.

  p2p application *p2p_list*: The supported applications are:

  - **8tracks**
  - **abcnetworks**
  - **actionvoip**
  - **actsync**
  - **adobeconnect**
  - **aimini**
  - **amazoncloud**
  - **amazonmusic**
  - **amazonvideo**
  - **antsp2p**
  - **apple-push**
  - **apple-store**
  - **applejuice**
  - **applemaps**
  - **ares**
  - **armagettron**
  - **avi**
  - **badoo**
  - **baidumovie**

- **battlefld**
- **bbm**
- **beatport**
- **betternet**
- **bitcasa**
- **bittorrent**
- **bittorrent-sync**
- **blackberry-store**
- **blackberry**
- **blackdialer**
- **box**
- **callofduty**
- **chikka**
- **cisco-jabber**
- **citrix**
- **clubbox**
- **clubpenguin**
- **crackle**
- **crossfire**
- **crunchyroll**
- **cyberghost**
- **ddlink**
- **deezer**
- **didi**
- **directconnect**
- **dish-anywhere**
- **disneymovies**
- **dofus**
- **dramafever**
- **dropbox**
- **edonkey**
- **espn**

- **expressvpn**
- **facebook**
- **facetime**
- **fandor**
- **fasttrack**
- **feidian**
- **fiesta**
- **filetopia**
- **filmontv**
- **flash**
- **flickr**
- **florensia**
- **foursquare**
- **fox-sports**
- **freenet**
- **friendster**
- **fring**
- **funshion**
- **gadu_gadu**
- **gamekit**
- **gmail**
- **gnutella**
- **go90**
- **goober**
- **google-music**
- **google-push**
- **google**
- **googleplay**
- **googleplus**
- **gotomeeting**
- **gtalk**
- **guildwars**

- **halflife2**
- **hamachivpn**
- **hayu**
- **hbogo**
- **hbonow**
- **heytell**
- **hgtv**
- **hike-messenger**
- **hls**
- **hotspotvpn**
- **hulu**
- **hyves**
- **iax**
- **icall**
- **icecast**
- **icloud**
- **idrive**
- **igo**
- **iheartradio**
- **imesh**
- **imessage**
- **imgur**
- **imo**
- **instagram**
- **iplayer**
- **iptv**
- **irc**
- **isakmp**
- **iskoot**
- **itunes**
- **jabber**
- **jap**

- **jumblo**
- **kakaotalk**
- **kik-messenger**
- **kontiki**
- **kugoo**
- **kuro**
- **linkedin**
- **livestream**
- **lync**
- **magicjack**
- **manolito**
- **mapfactor**
- **mapi**
- **maplestory**
- **meebo**
- **mgcp**
- **mlb**
- **mojo**
- **monkey3**
- **mozy**
- **msn**
- **msrp**
- **mute**
- **mypeople**
- **myspace**
- **nateontalk**
- **naverline**
- **navigon**
- **nbc-sports**
- **netmotion**
- **newsy**
- **nick**

- **nimbuzz**
- **nokia-store**
- **octoshape**
- **off**
- **ogg**
- **oist**
- **oovoo**
- **opendrive**
- **openft**
- **openvpn**
- **orb**
- **oscar**
- **outlook**
- **paltalk**
- **pando**
- **pandora**
- **path**
- **pbs**
- **pcanywhere**
- **periscope**
- **pinterest**
- **plingm**
- **poco**
- **popo**
- **pplive**
- **ppstream**
- **ps3**
- **qq**
- **qqgame**
- **qqlive**
- **quake**
- **quic**

- **quicktime**
- **radio-paradise**
- **radius**
- **rdp**
- **rdt**
- **regram**
- **rfactor**
- **rhapsody**
- **rmstream**
- **rodi**
- **rynga**
- **samsung-store**
- **scydo**
- **secondlife**
- **shoutcast**
- **showtime**
- **silverlight**
- **siri**
- **skinny**
- **skydrive**
- **skype**
- **slacker-radio**
- **slingbox**
- **slingtv**
- **smartvoip**
- **snapchat**
- **softether**
- **sopcast**
- **soribada**
- **soulseek**
- **soundcloud**
- **spark**

- **spdy**
- **speedtest**
- **spike**
- **splashfighter**
- **spotify**
- **ssdp**
- **starz**
- **stealthnet**
- **steam**
- **stun**
- **sudaphone**
- **svtplay**
- **tagged**
- **talkatone**
- **tango**
- **teamspeak**
- **teamviewer**
- **telegram**
- **thunder**
- **tinder**
- **tmo-tv**
- **tor**
- **truecaller**
- **truphone**
- **tumblr**
- **tunein-radio**
- **tunnelvoice**
- **turbovpn**
- **tvants**
- **tvland**
- **tvuplayer**
- **twitch**

- **twitter**
- **ultrabac**
- **ultrasurf**
- **univision**
- **upc-phone**
- **usenet**
- **ustream**
- **uusee**
- **vchat**
- **veohtv**
- **vessel**
- **vevo**
- **viber**
- **vine**
- **voipdiscount**
- **vopium**
- **vpnmaster**
- **vpnx**
- **voxer**
- **vtok**
- **vtun**
- **vudu**
- **warcft3**
- **waze**
- **webex**
- **wechat**
- **whatsapp**
- **wii**
- **windows-azure**
- **windows-store**
- **winmx**
- **winny**

- **wmstream**
- **wofkungfu**
- **wofwarcraft**
- **wuala**
- **xbox**
- **xdcc**
- **xing**
- **yahoo**
- **yahoomail**
- **yiptv**
- **youku**
- **yourfreetunnel**
- **youtube**
- **zattoo**

p2p protocol-group *group_list*: The following P2P protocol groups are supported:

- generic
- anonymous-access
- business
- communicator
- cloud
- e-store
- e-mail
- e-news
- internet-privacy
- filesharing
- gaming
- p2p-filesharing
- p2p-anon-filesharing
- remote-control
- social-nw-gaming
- social-nw-generic
- social-nw-videoconf
- standard
- streaming

wide [all]: Displays all available P2P statistics in a single wide line. The **all** keyword displays all available P2P statistics without suppressing zeroes.

- **pop3**
- **pptp**

- **rtcp**
- **rtp**
- **rtsp**
- **sdp**
- **secure-http**
- **sip**
- **smtp**
- **tcp**
- **tftp**
- **udp**
- **wsp**
- **wtp**

[instance *instance_number*]

Displays the ACS/Session Manager information for specific instances.

instance_number must be an integer from 1 through 65535.

verbose

Specifies to display detailed (all available) information. If not specified, concise information is displayed.

| { 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.

Usage Guidelines

Use this command to display statistic information for active charging protocol analyzers.

Example

The following command displays detailed statistic information for all P2P protocol analyzers:

```
show active-charging analyzer statistics name p2p verbose
```

The following command displays detailed statistic information for all TCP protocol analyzers:

```
show active-charging analyzer statistics name tcp verbose
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging bandwidth-policy

Displays information on bandwidth policies configured in a service.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show active-charging bandwidth-policy { all | name` *`bandwidth_policy_name`* **`} [ | { grep`** *`grep_options`* **`| more } ]`**

all

Displays information for all bandwidth policies configured in the service.

name *bandwidth_policy_name*

Displays detailed information for an existing bandwidth policy specified 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.

Usage Guidelines

Use this command to view information on bandwidth policies configured in a service.

Example

The following command displays detailed information for the bandwidth policy named *standard*:

`show active-charging bandwidth-policy name standard`

show active-charging charging-action

Displays information for charging actions configured in the Active Charging Service (ACS).

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show active-charging charging-action { { { all | name` *`charging_action_name`* **} [service name** *`acs_service_name`* **] } | statistics [name** *`charging_action_name`* **] } [| { grep** *`grep_options`* **| more }]**

all

Displays information for each configured charging action.

name *charging_action_name*

Displays detailed information for an existing charging action specified as an alphanumeric string of 1 through 63 characters.

statistics

Displays statistical information for all configured charging actions.

service name *acs_service_name*

Displays information for all or a specific charging action in the specified ACS. *acs_service_name* is an alphanumeric string of 1 through 15 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.

Usage Guidelines

Use this command to display information for charging actions configured in a service.

Example

The following command displays a detailed information for all charging actions:

```
show active-charging charging-action all
```

Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging content-filtering category policy-id

Displays Content Filtering (CF) category policy definitions.

Product CF

Privilege Security Administrator, Administrator, Operator, Inspector

Command Modes Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description **`show active-charging content-filtering category policy-id { all | id`** *`policy_id`* **`} [ | { grep`** *`grep_options`* **`| more } ]`**

all

Displays definitions of all Content Filtering category policies.

id *policy_id*

Displays definitions of an existing Content Filtering category policy specified as an integer from 1 through 4294967295.

| { grep *grep_options* | more }

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

Usage Guidelines Use this command to view Content Filtering category definitions for a specific/all Policy IDs.

Example

The following command displays Content Filtering category definitions for policy ID *3*:

```
show active-charging content-filtering category policy-id id 3
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging content-filtering category statistics

Displays category-based content filtering statistics.

Product CF

Privilege Security Administrator, Administrator, Operator, Inspector

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show active-charging content-filtering category statistics [rulebase { name *rulebase_name* **| all }] [verbose] [| { grep** *grep_options* **| more }]**

rulebase { name *rulebase_name* | all }

Displays category-based content filtering statistics, either for all or for a specific rulebase.

- **name** *rulebase_name*: Specifies an existing rulebase as an alphanumeric string of 1 through 63 characters.
- **all**: Displays category-based content filtering statistics for each rulebase in the ACS.

verbose

Specifies to display detailed (all available) information. If not specified, concise information is displayed.

| { grep *grep_options* | more }

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

Usage Guidelines

Use this command to view category-based content filtering statistics for a specific rulebase, or cumulative statistics for all rulebases in the ACS.

Note From Release 21.4, the following changes are made to the output of this show command:

- The "Total number of successful Cache lookups" field is excluded.
- The **> 50ms** value is excluded from the “Time taken for rating” field.
- The following sub-fields are added to the “Time taken for rating” field:
  - 50-100ms
  - 100-200ms
  - 200-300ms
  - 300ms

Example

The following command displays category-based content filtering statistics for the rulebase named *consumer*:

show active-charging content-filtering category statistics rulebase name *consumer*

The following command displays cumulative category-based content filtering statistics for all rulebases in verbose mode:

show active-charging content-filtering category statistics verbose

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging content-filtering server-group

Displays information for Content Filtering Server Group (CFSG) configured in the service.

Product

CF

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

show active-charging content-filtering server-group [name *cfsg_name* **| statistics [name** *cfsg_name* **[acsmgr instance** *instance_number* **[priority** *priority* **]] | verbose] [| { grep** *grep_options* **| more }]**

name *cfsg_name*

Specifies name of an existing CFSG as an alphanumeric string of 1 through 63 characters.

acsmgr instance *instance_number*

Specifies the manager instance as an integer from 1 through 65535.

priority *priority*

Specifies the priority of the server for which statistics has to be displayed as an integer from 1 through 65535.

verbose

Specifies to display detailed (all available) information, for each ICAP server connection at each instance. If not specified, concise information is displayed.

| { grep *grep_options* | more }

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

Usage Guidelines

Use this command to view CFSG information/statistics.

show active-charging content-filtering server-group name *cfsg_name*: The output of this command displays detailed information for the specified CFSG.

show active-charging content-filtering server-group statistics name *cfsg_name*: The output of this command displays cumulative statistics for the specified CFSG. This will include all the instances and all the servers configured in the CFSG.

show active-charging content-filtering server-group statistics name *cfsg_name* **acsmgr instance** *instance_number*: The output of this command displays the cumulative statistics of all the ICAP server connections on the specified manager instance.

show active-charging content-filtering server-group statistics name *cfsg_name* **acsmgr instance** *instance_number* **priority** *priority*: The output of this command displays the statistics for the specified ICAP server connection on the specified manager instance.

show active-charging content-filtering server-group statistics verbose: The output of this command displays statistics of each ICAP server connection at each instance.

Example

The following command displays information for the CFSG named *test12*:

```
show active-charging content-filtering server-group name test12
```

The following command displays detailed information for all CFSGs:

```
show active-charging content-filtering server-group statistics verbose
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging credit-control

Displays statistics for Diameter/RADIUS Prepaid Credit Control Service in the Active Charging Service (ACS).

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show active-charging credit-control { misc-info max-backpressure [ all |
 facility sessmgr instance instance_number ] | statistics [ group group_name
| server { all | ip-address ip_address [ port port_num ] | name server_name }
] | session-states [ rulebase rulebase_name ] [ content-id content_id ] } [ |
 { grep grep_options | more } ]
```

misc-info max-backpressure [all | facility sessmgr instance *instance_number*]

Displays miscellaneous information including the maximum backpressure hit count for all active session managers.

- **all**: Displays the max-backpressure count from all session manager instances.
- **facility sessmgr instance** *instance_number*: Displays logged events for specific facility. That is, it will display the maximum backpressure count on that specific session manager instance.

  The session manager instance number must be an integer ranging from 1 through 65535 characters.

statistics [group *group_name* | server { all | ip-address *ip_address* [port *port_num*] | name *server_name* }]

Displays prepaid credit control statistics.

- **group** *group_name*: Displays statistics for an existing credit control group specified as an alphanumeric string of 1 through 63 characters.
- **server { all | ip-address** *ip_address* **[port** *port_num* **] | name** *server_name* **}]**: Displays statistics for the specified credit control server.
  - **all**: Displays all available statistics including host statistics.
  - **ip-address** *ip_address*: Displays available statistics for the specified server's address.
  - **port** *port_num*: Displays available statistics for the specified server's port number.
  - **name** *server_name*: Displays the credit control statistics for the specified server.

session-states [rulebase *rulebase_name*] [content-id *content_id*]

Displays prepaid CCA session status based on rulebase and/or content ID.

- **rulebase** *rulebase_name*: Displays the Credit Control Application (CCA) session state counts for an existing rulebase specified as an alphanumeric string of 1 through 63 characters.
- **content-id** *content_id*: Displays CCA session state counts for a content ID of a credit control service specified as an integer from 1 through 65535.

| { grep *grep_options* | more }

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

Usage Guidelines

Use this command to view statistics for Diameter/RADIUS prepaid credit control service in the ACS.

Example

The following command shows ACS statistics of configured Diameter or RADIUS Credit Control Application:

```
show active-charging credit-control statistics
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging dns-learnt-ip-addresses

Displays DNS learnt IP address statistics for the DNS Snooping feature.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show active-charging dns-learnt-ip-addresses statistics { sessmgr { all | instance` *`sessmgr_instance_number`* **`} [ verbose ] | summary } [ | { grep`** *`grep_options`* **`| more } ]`**

sessmgr { all | instance *sessmgr_instance_number* } [verbose]

Displays information for all or the specified Session Manager (SessMgr) instance.

- **all**: Displays information for all SessMgr instances.
- **instance** *sessmgr_instance_number*: Displays information for a SessMgr instance specified as an integer from 1 through 65535.
- **verbose**: Displays detailed statistics for specified criteria. Use this keyword to view the learnt IP addresses.

summary

Displays summary information.

| { grep *grep_options* | more }

Specifies that the output of this command is to be piped (sent) to the command specified. You must specify a command to which the output 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.

Usage Guidelines

Use this command to view statistics for the DNS Snooping feature related DNS learnt-ip-addresses.

This command displays the number of learnt IP entries per rule line. It displays on a service level the number of resolved (learnt) IP addresses per rule line per rulebase (once if a rule line is used multiple times in the same rulebase as it is shared across rulebase) per destination context per SessMgr instance. It also displays the number of entries flushed due to TTL expiry. The field entries_replaced gives the number of entries replaced (same IP returned again) in the pool due to a DNS response by same/another subscriber for same domain-name, wherein the TTL of the entry will be replaced.

IPv4-overflows will start incrementing when the maximum limit of 51200 across system is reached OR limit of 200 per pattern is reached.

Ipv6-overflows will start incrementing when maximum limit of 25600 across system is reached OR limit of 100 per pattern is reached.

Limits are:

- Maximum of 51,200 IPv4 entries per instance shared across IPv4 all pools.
- Maximum of 200 IPv4 entries per pool (pool is same as discussed before (per rule-line pattern)).
- Maximum of 25,600 IPv6 entries per instance shared across all IPv6 pools.
- Maximum of 100 IPv6 entries per pool.

In releases prior to 14.0, this CLI command **show active-charging dns-learnt-ip statistics sessmgr all** displayed all the configured patterns and rulebase names for each of the pattern entry, even though the pattern has not learnt any IP address. When a large number of DNS snooping ruledefs are configured (configured as ip server-domain name under ruledef configuration), the memory allocated for sending this information exceeded the message size limit for messenger calls and hence the crash was observed.

To avoid the crash occuring, in 14.0 and later releases, the output of the CLI command **show active-charging dns-learnt-ip statistics sessmgr all**is modified to display only the patterns for which at least one IPv4/IPv6 address is learnt as all other information is available from the configuration. Also for each of the patterns this CLI command will not be displaying rulebase name as it can be printed once.

Example

The following command displays summary statistics for DNS learnt IP addresses:

```
show active-charging dns-learnt-ip-addresses statistics summary
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging edr-format

Displays information about Event Data Record (EDR) formats configured in the Active Charging Service (ACS).

Product ACS

Privilege Security Administrator, Administrator, Operator, Inspector

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show active-charging edr-format [ statistics ] [ all | name edr_format_name ] [ | { grep grep_options | more } ]
```

all

Displays information for all EDR formats.

statistics

Displays statistics for all or an existing EDR format.

If neither **all** nor **name** is specified, summarized statistics over all EDR formats is displayed.

name *edr_format_name*

Displays information for an existing EDR format specified 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 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.

Usage Guidelines

Use this command to display information for EDR format(s) in the ACS.

Example

The following command displays all configured EDR formats in the ACS.

```
show active-charging edr-format all
```

Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging edr-udr-file

Displays CDR flow control information. This command also displays the Event Data Record (EDR) and Usage Data Record (UDR) file information.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show active-charging edr-udr-file { flow-control-counters [ verbose ] |
statistics } [ | { grep grep_options | more } ]
```

flow-control-counters [verbose]

Displays the counters for dropped EDR/UDR records. These counters are for when CDRMOD uses flow control to stop ACS/Session Managers from sending the records.

verbose displays detailed information.

statistics

Important This keyword is obsolete. The option is now supported through the **show cdr** command.

Displays EDR and UDR file statistics.

| { 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.

Usage Guidelines Use this command to view CDR flow control information.

Example

The following command displays EDR and UDR files statistics:

```
show active-charging edr-udr-file statistics
```

The following command displays CDR flow control information:

```
show active-charging edr-udr-file flow-control-counters
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging file-space-usage

Displays the file space used by Charging Data Record (CDR) and Event Data Record (EDR) files.

Product ACS

Privilege Security Administrator, Administrator, Operator, Inspector

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description `show active-charging file-space-usage [ | { grep grep_options | more } ]`

| { grep *grep_options* | more }

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

Usage Guidelines Use this command to view CDR/EDR file space usage information. The context in which this command is used is not relevant.

Example

The following command displays CDR/EDR file space usage:

```
show active-charging file-space-usage
```

show active-charging firewall dos-protection

Displays the list of servers involved in any IP Sweep attacks.

Product PSF

Privilege Security Administrator, Administrator, Operator, Inspector

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description `show active-charging firewall dos-protection ip-sweep server-list { all | instance instance_num } [ | { grep grep_options | more }`

all

Displays the IP Sweep server list for all instances.

instance *instance_num*

Displays statistics for the specified ACS Manager instance.

instance_num must be an integer from 1 through 65535.

| { grep *grep_options* | more }

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

Usage Guidelines Use this command to display the list of servers involved in any IP Sweep attacks.

Example

The following command displays the IP Sweep server list for all instances:

```
show active-charging firewall dos-protection ip-sweep server-list all
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging firewall statistics

Displays Active Charging Stateful Firewall statistics.

Product PSF

Privilege Security Administrator, Administrator, Operator, Inspector

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show active-charging firewall statistics [ callid call_id | domain-name
domain_name | nat-realm nat_realm_name | protocol { icmp | icmpv6 | ip | ipv6
 | other | tcp | udp } | username user_name ] [ acsmgr instance instance_number
 ] [ verbose ] [ wide ] [ | { grep grep_options | more } ]
```

acsmgr instance *instance_number*

Specifies the ACS/Session Manager instance ID as an integer from 1 through 65535.

callid *call_id*

Specifies the call identification number as an 8-digit hexadecimal number.

domain-name *domain_name*

Specifies the domain name as an alphanumeric string of 1 through 127 characters.

nat-realm *nat_realm_name*

Specifies the NAT realm name as an alphanumeric string of 1 through 31 characters.

protocol { icmp | ip | other | tcp | udp }

Specifies the protocol:

- **icmp**: ICMPv4

- **icmpv6**
- **ip**: IPv4
- **ipv6**
- **other**: Protocols other than TCP, UDP, and ICMPv4/ICMPv6.
- **tcp**
- **udp**

username *user_name*

Specifies the user name as an alphanumeric string of 1 through 127 characters.

verbose

Specifies to display detailed (all available) information. If not specified, concise information is displayed.

wide

Displays all available information in a single wide line.

| { grep *grep_options* | more }

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

Usage Guidelines

Use this command to view Stateful Firewall statistics. If you are in the local context, statistics for all contexts are displayed. Otherwise, only statistics of your current context are displayed.

Example

The following command displays Stateful Firewall statistics:

```
show active-charging firewall statistics
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging firewall track-list

Displays the list of servers being tracked for involvement in any Denial-of-Service (DOS) attacks.

Product

PSF

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show active-charging firewall track-list attacking-servers [ | { grep` *`grep_options`* **`| more } ]`**

| { grep *grep_options* | more }

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

Usage Guidelines

Use this command to view details of servers being tracked for involvement in any DOS attack.

Example

The following command displays the list of servers being tracked for involvement in any DOS attacks:

`show active-charging firewall track-list attacking-servers`

Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging flow-control-counters

Displays information for dropped EDR and UDR records.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show active-charging flow-control-counters [ verbose ] [ | { grep` *`grep_options`* **`| more } ]`**

verbose

Specifies to display detailed (all available) information. If not specified, concise information is displayed.

| { grep *grep_options* | more }

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

Usage Guidelines

Use this command to view EDR-UDR flow control information—for dropped EDR and UDR records.

Example

The following command displays detailed EDR-UDR flow control information:

```
show active-charging flow-control-counters verbose
```

Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging flow-kpi

Displays information about the cumulative KPI for ECS rule(s) across session managers.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show active-charging flow-kpi sessmgr { all | instance instance_id } [ | { grep grep_options | more } ]
```

all

Displays the KPI information for all rules.

instance *instance_id*

Displays information for all rules based on session manager instance, specified as an integer ranging from 1 through 65535.

| { grep *grep_options* | more }

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

Usage Guidelines

Use this command to view the cumulative KPI for ECS rule(s) across session managers.

This command is added in support of the Flow Recovery feature, that requires a separate feature license.

Example

The following command displays the KPI information for all rules:

```
show active-charging flow-kpi all
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging flow-mappings

Displays information about all the active flow mappings based on the applied filters.

Product

PSF

NAT

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show active-charging flow-mappings [ all | call-id call_id | [ nat {
not-required | required [ nat-realm nat_realm_name ] } | trans-proto { tcp
| udp } ] + [ | { grep grep_options | more } ]
```

all

Displays all the available active-charging flow-mapping information.

call-id *call_id*

Displays detailed information for a call ID specified as an 8-digit hexadecimal number.

nat { required [nat-realm *string*] not-required }

Displays the active charging flow mappings for which NAT is enabled or disabled.

trans-proto { tcp | udp }

Displays the transport layer.

| { grep *grep_options* | more }

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

Usage Guidelines

Use this command to view the Active Charging flow-mapping details.

Example

The following command displays the total number of Active Charging flow-mappings:

```
show active-charging flow-mappings all
```

The following command displays the flow-mappings for which NAT is enabled and the NAT-realm used is *natpool3*:

```
show active-charging flow-mappings nat required nat-realm natpool3
```

Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging flows

Displays information for active charging flows.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show active-charging flows { all | [ callid call_id ] [ connected-time [ < | > | greater-than | less-than ] seconds ] [ control-connection { ftp | pptp | rtsp | sip | tftp } ] [ flow-id flow_id ] [ full ] [ idle-time [ < | > | greater-than | less-than ] seconds ] [ firewall { not-required | required } ] [ imsi imsi_value ] [ ip-address [ server | subscriber ] [ < | > | IPv4 | greater-than | less-than ] address ] [ msisdn msisdn_num ] [ nat { not-required | required [ nat-ip nat_ip_address ] [ binding-info ] } ] [ pacing-bitrate [ < | > | = | greater-than | less-than | equal-to ] number [ port-number [ server | subscriber ] [ < | > | IPv4 | greater-than | less-than ] number ] [ rx-bytes [ < | > | greater-than | less-than ] number ] [ rx-packets [ < | > | greater-than | less-than ] number ] [ session-id session_id ] [ summary ] [ trans-proto { icmp | tcp | udp } ] [ tx-bytes [ < | > | greater-than | less-than ] number ] [ tx-packets [ < | > |
```

greater-than | less-than] *number* **] [type** *flow_type* **] [username** *user_name* **] } [| { grep** *grep_options* **| more }]**

all

Displays information for all active charging flows.

callid *call_id*

Displays the specific Call Identification Number. *call_id* must be an eight digit hexadecimal number.

connected-time [< | > | greater-than | less-than] *seconds*

Displays information for flows filtered by connected time period.

- < *seconds*: Displays flows that have been connected less than the specified number of seconds.
- > *seconds*: Displays flows that have been connected more than the specified number of seconds.
- **greater-than** *seconds*: Displays flows that have been connected more than the specified number of seconds.
- **less-than** *seconds*: Displays flows that have been connected less than the specified number of seconds.

seconds is an integer from 0 through 4294967295.

control-connection { ftp | pptp | rtsp | sip | tftp }

Displays information for control connection of flows.

- **ftp**: Displays control connection information for the FTP flow.
- **pptp**: Displays control connection information for the PPTP flow.
- **rtsp**: Displays control connection information for the RTSP flow.
- **sip**: Displays control connection information for the SIP flow.
- **tftp**: Displays control connection information for the TFTP flow.

firewall { not-required | required }

Displays information for flows filtered by Firewall required or not required setting.

- **not-required**: Sessions with Firewall processing are not required.
- **required**: Sessions with Firewall processing are required.

flow-id *flow_id*

Displays concise information for specified active charging flow ID.

full

Displays all available information for the specified flows.

idle-time [< | > | greater-than | less-than] *seconds*

Displays information for flows filtered by idle time period.

- < *seconds*: Displays flows that have been idle less than the specified number of seconds.
- > *seconds*: Displays flows that have been idle more than the specified number of seconds.
- **greater-than** *seconds*: Displays flows that have been idle more than the specified number of seconds.
- **less-than** *seconds*: Displays flows that have been idle less than the specified number of seconds.

seconds is an integer from 0 through 4294967295.

imsi *imsi_value*

Displays information for an International Mobile Subscriber Identity (IMSI). *imsi_value* must be a sequence of digits and/or wild characters.

ip-address [server | subscriber] [< | > | IPv4 | greater-than | less-than] *address*

Displays information for flows filtered by IPv4 IP address.

- **server**: Specifies the IP address for a specific server.
- **subscriber**: Displays subscriber details for the IP address specified in IPv4 dotted-decimal format.
- < *address*: Specifies an IPv4 IP address that is less than *address*.
- > *address*: Specifies an IPv4 IP address that is greater than *address*.
- **greater-than** *address*: Specifies an IPv4 IP address that is greater than *address*.
- **less-than** *address*: Specifies an IPv4 IP address that is less than *address*.

address is an IP address expressed in IPV4 dotted-decimal notation.

msisdn *msisdn_num*

Displays information for the mobile user identified by the Mobile Subscriber ISDN Number (MSISDN). *msisdn_num* must be a numeric string of 1 to 15 digits.

nat { not-required | required [nat-ip *nat_ip_address* [nat-port *nat_port*]] [binding-info] }

Important The **nat** keyword and options are only available in StarOS 8.3 and later releases.

Displays information for flows filtered by Network Address Translation (NAT) required or not required setting.

- **not-required**: Sessions with NAT processing are not required.
- **required**: Sessions with NAT processing are required.
- **nat-ip** *nat_ip_address*: Sessions using the NAT IP address expressed in IPv4 dotted-decimal notation.

- **nat-port** *nat_port*: Sessions using the specified NAT IP address and NAT port number specified as an integer from 0 through 65535.
- **binding-info**: Displays the NAT binding information of the NATed flow.

pacing-bitrate [< | > | = | greater-than | less-than | equal-to] *number*

Displays information on video flows filtered by a video pacing bit rate specified an integer from 1 to 256000000.

- < *number*: Specifies a number that is less than the specified video pacing bit rate.
- > *number*: Specifies a number that is greater than the specified video pacing bit rate.
- = *number*: Specifies a number that is equal to the specified video pacing bit rate.
- **greater-than** *number*: Specifies a number that is greater than the specified video pacing bit rate.
- **less-than** *number*: Specifies a number that is less than the specified video pacing bit rate
- **equal-to** *number*: Specifies a number that is equal to the specified video pacing bit rate.

port-number [server | subscriber] [< | > | IPv4 | greater-than | less-than] _*number*

Displays information on flows filtered by port number.

- **server**: Specifies the port-number for a specific server.
- **subscriber**: Specifies subscriber details for this port-number, and must be an integer from 0 through 65535.
- < *number*: Specifies a port number that is less than the specified port-number.
- > *number*: Specifies a port number that is greater than the specified port-number.
- **greater-than** *number*: Specifies a port number that is greater than the specified port-number.
- **less-than** *number*: Specifies a port number that is less than the specified port-number.

rx-bytes [< | > | greater-than | less-than] *number*

Displays information on flows filtered by the number of bytes received in the flow.

- < *number*: Specifies the number of bytes that is less than the specified rx-bytes.
- > *number*: Specifies number of bytes that is greater than the specified rx-bytes.
- **greater-than** *number*: Specifies number of bytes that is greater than the specified rx-bytes.
- **less-than** *number*: Specifies number of bytes that is less than the specified rx-bytes.

number must be an integer from 0 through 18446744073709551615.

rx-packets [< | > | greater-than | less-than] *number*

Displays information on flows filtered by the number of packets received in the flow.

- **greater-than** *number*: Specifies the number of packets that is greater than the specified rx-packets.

- **less-than** *number*: Specifies the number of packets that is less than the specified rx-packets.

number must be an integer from 0 through 18446744073709551615.

session-id *session_id*

Displays detailed information for specific active charging session ID.

summary

Displays summary information for defined sessions, based on defined parameters.

trans-proto { icmp | tcp | udp }

Displays information on flows filtered by the transport protocol.

- **icmp**: ICMP protocol type flow
- **tcp**: TCP protocol type flow
- **udp**: User Datagram Protocol (UDP) flows

tx-bytes [< | > | greater-than | less-than] *number*

Displays information on flows filtered by the number of bytes received in the flow.

- < *number*: Specifies the number of bytes that is less than the specified tx-bytes.
- > *number*: Specifies number of bytes that is greater than the specified tx-bytes.
- **greater-than** *number*: Specifies number of bytes that is greater than the specified tx-bytes.
- **less-than** *number*: Specifies number of bytes that is less than the specified tx-bytes.

number must be an integer from 0 through 18446744073709551615.

tx-packets [< | > | greater-than | less-than] *number*

Displays information on flows filtered by the number of packets received in the flow.

- **greater-than** *number*: Specifies the number of packets that is greater than the specified tx-packets.
- **less-than** *number*: Specifies the number of packets that is less than the specified tx-packets.

number must be an integer from 0 through 18446744073709551615.

type *flow_type*

Displays information on flows filtered by flow type of application protocol.

flow_type must be one of the following:

- **dns**
- **ftp**
- **http**

- **icmp**
- **icmpv6**
- **imap**
- **ip**
- **ipv6**
- **mms**
- **p2p [application** *p2p_list* **[traffic-type** *traffic_type* **] | protocol-group** *group_list* **]**: Peer-to-peer analyzer.

  p2p application *p2p_list*: P2P protocol type flows include one or more of the following applications:

  - **8tracks**
  - **abcnetworks**
  - **actionvoip**
  - **actsync**
  - **adobeconnect**
  - **aimini**
  - **amazoncloud**
  - **amazonmusic**
  - **amazonvideo**
  - **antsp2p**
  - **apple-push**
  - **apple-store**
  - **applejuice**
  - **applemaps**
  - **ares**
  - **armagettron**
  - **avi**
  - **badoo**
  - **baidumovie**
  - **battlefld**
  - **bbm**
  - **beatport**
  - **betternet**

- **bitcasa**
- **bittorrent**
- **bittorrent-sync**
- **blackberry-store**
- **blackberry**
- **blackdialer**
- **box**
- **callofduty**
- **chikka**
- **cisco-jabber**
- **citrix**
- **clubbox**
- **clubpenguin**
- **crackle**
- **crossfire**
- **crunchyroll**
- **cyberghost**
- **ddlink**
- **deezer**
- **didi**
- **directconnect**
- **dish-anywhere**
- **disneymovies**
- **dofus**
- **dramafever**
- **dropbox**
- **edonkey**
- **espn**
- **expressvpn**
- **facebook**
- **facetime**
- **fandor**

- **fasttrack**
- **feidian**
- **fiesta**
- **filetopia**
- **filmontv**
- **flash**
- **flickr**
- **florensia**
- **foursquare**
- **fox-sports**
- **freenet**
- **friendster**
- **fring**
- **funshion**
- **gadu_gadu**
- **gamekit**
- **gmail**
- **gnutella**
- **go90**
- **goober**
- **google-music**
- **google-push**
- **google**
- **googleplay**
- **googleplus**
- **gotomeeting**
- **gtalk**
- **guildwars**
- **halflife2**
- **hamachivpn**
- **hayu**
- **hbogo**

- **hbonow**
- **heytell**
- **hgtv**
- **hike-messenger**
- **hls**
- **hotspotvpn**
- **hulu**
- **hyves**
- **iax**
- **icall**
- **icecast**
- **icloud**
- **idrive**
- **igo**
- **iheartradio**
- **imesh**
- **imessage**
- **imgur**
- **imo**
- **instagram**
- **iplayer**
- **iptv**
- **irc**
- **isakmp**
- **iskoot**
- **itunes**
- **jabber**
- **jap**
- **jumblo**
- **kakaotalk**
- **kik-messenger**
- **kontiki**

- **kugoo**
- **kuro**
- **linkedin**
- **livestream**
- **lync**
- **magicjack**
- **manolito**
- **mapfactor**
- **mapi**
- **maplestory**
- **meebo**
- **mgcp**
- **mlb**
- **mojo**
- **monkey3**
- **mozy**
- **msn**
- **msrp**
- **mute**
- **mypeople**
- **myspace**
- **nateontalk**
- **naverline**
- **navigon**
- **nbc-sports**
- **netmotion**
- **newsy**
- **nick**
- **nimbuzz**
- **nokia-store**
- **octoshape**
- **off**

- **ogg**
- **oist**
- **oovoo**
- **opendrive**
- **openft**
- **openvpn**
- **orb**
- **oscar**
- **outlook**
- **paltalk**
- **pando**
- **pandora**
- **path**
- **pbs**
- **pcanywhere**
- **periscope**
- **pinterest**
- **plingm**
- **poco**
- **popo**
- **pplive**
- **ppstream**
- **ps3**
- **qq**
- **qqgame**
- **qqlive**
- **quake**
- **quic**
- **quicktime**
- **radio-paradise**
- **radius**
- **rdp**

- **rdt**
- **regram**
- **rfactor**
- **rhapsody**
- **rmstream**
- **rodi**
- **rynga**
- **samsung-store**
- **scydo**
- **secondlife**
- **shoutcast**
- **showtime**
- **silverlight**
- **siri**
- **skinny**
- **skydrive**
- **skype**
- **slacker-radio**
- **slingbox**
- **slingtv**
- **smartvoip**
- **snapchat**
- **softether**
- **sopcast**
- **soribada**
- **soulseek**
- **soundcloud**
- **spark**
- **spdy**
- **speedtest**
- **spike**
- **splashfighter**

- **spotify**
- **ssdp**
- **starz**
- **stealthnet**
- **steam**
- **stun**
- **sudaphone**
- **svtplay**
- **tagged**
- **talkatone**
- **tango**
- **teamspeak**
- **teamviewer**
- **telegram**
- **thunder**
- **tinder**
- **tmo-tv**
- **tor**
- **truecaller**
- **truphone**
- **tumblr**
- **tunein-radio**
- **tunnelvoice**
- **turbovpn**
- **tvants**
- **tvland**
- **tvuplayer**
- **twitch**
- **twitter**
- **ultrabac**
- **ultrasurf**
- **univision**

- **upc-phone**
- **usenet**
- **ustream**
- **uusee**
- **vchat**
- **veohtv**
- **vessel**
- **vevo**
- **viber**
- **vine**
- **voipdiscount**
- **vopium**
- **vpnmaster**
- **vpnx**
- **voxer**
- **vtok**
- **vtun**
- **vudu**
- **warcft3**
- **waze**
- **webex**
- **wechat**
- **whatsapp**
- **wii**
- **windows-azure**
- **windows-store**
- **winmx**
- **winny**
- **wmstream**
- **wofkungfu**
- **wofwarcraft**
- **wuala**

- **xbox**
- **xdcc**
- **xing**
- **yahoo**
- **yahoomail**
- **yiptv**
- **youku**
- **yourfreetunnel**
- **youtube**
- **zattoo**

traffic-type *traffic_type*: P2P protocol flows include the following traffic type classifications:

Important The traffic type for a P2P protocol may vary depending on the P2P protocol.

- **ads**
- **audio**
- **file-transfer**
- **im**
- **video**
- **voipout**
- **unclassified**

p2p protocol-group *group_list*: The following P2P protocol groups are supported:

- generic
- anonymous-access
- business
- communicator
- cloud
- e-store
- e-mail
- e-news
- internet-privacy
- filesharing
- gaming
- p2p-filesharing
- p2p-anon-filesharing

- remote-control
- social-nw-gaming
- social-nw-generic
- social-nw-videoconf
- standard
- streaming

- **pop3**
- **pptp**
- **rtcp**
- **rtp**
- **rtsp**
- **secure-http**
- **sip**
- **smtp**
- **tcp**
- **tftp**
- **udp**
- **unknown**: Unknown type of protocol type flow not listed here.
- **wsp-connection-less**
- **wsp-connection-oriented**

username *user_name*

Specifies the user name as a sequence of characters and/or wildcard characters ($ and *). *user_name* must be an alphanumeric string of 1 through 127 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 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.

Usage Guidelines

Use this command to display charging flow type information.

Example

The following command displays a detailed flow information for a session ID of *test*:

```
show active-charging flows session-id test
```

The following command displays a detailed flow information for a P2P type session:

show active-charging flows full type p2p

The following command displays a detailed information for a P2P type flow:

show active-charging flows type p2p

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging fw-and-nat policy

Displays Firewall-and-NAT Policy information.

Important This command is only available in StarOS 8.1, and in StarOS 9.0 and later. For more information on this command please contact your local service representative.

Product

ACS

PSF

NAT

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

show active-charging fw-and-nat policy { { { all | name *fw_nat_policy_name* **} [service name** *acs_service_name* **] } | { statistics { all | name** *fw_nat_policy_name* **} } } [| { grep** *grep_options* **| more }]**

all

Displays information for all Firewall-and-NAT policies configured, optionally all in a specified service.

name *fw_nat_policy_name*

Displays detailed information for an existing Firewall-and-NAT policy specified as an alphanumeric string of 1 through 63 characters.

service name *acs_service_name*

Displays information for all or the specified Firewall-and-NAT policy in the specified ACS.

acs_service_name must be the name of the active-charging service, and must be an alphanumeric string of 1 through 15 characters.

statistics

Displays statistics for all or the specified Firewall-and-NAT policy.

| { grep *grep_options* | more }

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

Usage Guidelines

Use this command to view Firewall-and-NAT Policy information.

Example

The following command displays detailed information for the Firewall-and-NAT policy named *standard*:

```
show active-charging fw-and-nat policy name standard
```

show active-charging group-of-objects

Displays information for ACS group-of-objects.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show active-charging group-of-objects { all | name group_of_objects_name } [
 | { grep grep_options | more } ]
```

all

Displays details of all group-of-objects configured in the system.

name *group_of_objects_name*

Displays details for the specified group-of-objects.

group_of_objects_name must be the name of a group-of-objects, and must be 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 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.

Usage Guidelines

Use this command to view information for all/specific group-of-objects.

Example

The following command displays information for a group-of-objects named *test*.

```
show active-charging group-of-objects name test
```

Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging group-of-prefixed-urls

D displays information on group of prefixed URLs configured in an Active Charging Service (ACS).

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show active-charging group-of-prefixed-urls { all | name *prefixed_url_group* **} [service name** *acs_service_name* **] [| { grep** *grep_options* **| more }]**

all

Displays information for all group of prefixed URLs configured in an ACS.

name *prefixed_url_group*

Displays detailed information for the group of prefixed URLs specified as an alphanumeric string of 1 through 63 characters.

service name *acs_service_name*

Displays information for all or the specified group of prefixed URLs in the specified ACS. *acs_service_name* must be the name of the ACS expressed as alphanumeric string of 1 through 15 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 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

Usage Guidelines Use this command to view information on group of prefixed URLs configured in the ACS.

Example

The following command displays for the group of prefixed URLs named *test123*:

```
show active-charging group-of-prefixed-urls name test123
```

show active-charging group-of-ruledefs

Displays information for all groups or a specified group of ruledefs configured in the Active Charging Service (ACS).

Product ACS

Privilege Security Administrator, Administrator, Operator, Inspector

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show active-charging group-of-ruledefs { { all | name group_of_ruledefs_name
 } [ service name acs_service_name ] | statistics name group_of_ruledefs_name }
[ | { grep grep_options | more } ]
```

all

Displays information for all groups of ruledefs configured, optionally all in a specified ACS.

name *group_of_ruledefs_name*

Displays detailed information for an existing group of ruledefs specified as an alphanumeric string of 1 through 63 characters.

service name *acs_service_name*

Displays information for all groups or the specified group of ruledefs within the ACS. *acs_service_name* must be the name of the ACS, and must be an alphanumeric string of 1 through 15 characters.

statistics name *group_of_ruledefs_name*

Displays statistics for an existing group of ruledefs specified 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 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.

Usage Guidelines

Use this command to view information on group of ruledefs configured in a ACS.

Example

The following command displays information on all groups of ruledefs configured:

```
show active-charging group-of-ruledefs all
```

show active-charging nat statistics

Displays Network Address Translation (NAT) realm statistics.

Product

NAT

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show active-charging nat statistics [instance *instance_number* **| nat-realm** *nat_realm_name* **[summary] | unsolicited-pkts-server-list [instance** *instance_number* **]] [| { grep** *grep_options* **| more }]**

show active-charging nat statistics

When issued in the local context, this command displays statistics for all NAT realms in all contexts. When issued in a specific context, this command displays statistics for all NAT realms in that context.

show active-charging nat statistics instance *instance_number*

When issued in the local context, this command displays statistics for the specified ACS/Session Manager instance in all contexts. When issued in a specific context, this command displays statistics for the specified ACS/Session Manager instance in that context.

show active-charging nat statistics nat-realm *nat_realm_name*

When issued in the local context, this command displays statistics for the specified NAT realm in all contexts. When issued in a specific context, this command displays statistics for the specified NAT realm in that context.

show active-charging nat statistics unsolicited-pkts-server-list instance *instance_num*

When issued in the local context, this command displays statistics for unsolicited packets in all contexts. When issued in a specific context, this command displays statistics for unsolicited packets that context.

instance_number must be an integer from 1 through 65535.

nat-realm *nat_realm_name*

Specifies the NAT realm's / NAT realm group's name.

nat_realm_name must be an alphanumeric string of 1 through 31 characters.

instance *instance_number*

Displays statistics for the specified ACS/Session Manager instance.

instance_number must be an integer from 1 through 65535.

summary

When the *nat_realm_name* specified is a "pool group" and the **summary** option is used, summary statistics of all pools in the pool group are displayed.

When the *nat_realm_name* specified is a pool and the **summary** option is not used, all available statistics for the specified pool are displayed.

When the *nat_realm_name* specified is a "pool group" and the **summary** option is not used, all available statistics of each pool in the specified "pool group" are displayed.

unsolicited-pkts-server-list

Displays statistics with the list of servers from where most number of unsolicited packets are received for the specified ACS/Session Manager instance.

| { grep *grep_options* | more }

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

Usage Guidelines

Use this command to view NAT realm statistics.

Example

The following command when issued in the local context, displays NAT realm statistics for NAT realms named *test135* in all contexts:

```
show active-charging nat statistics nat-realm test135
```

show active-charging p2p-dynamic-rules

This command is under development for a future release and is not supported in this release. This command displays P2P Dynamic signature file information.

Product

ADC

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show active-charging p2p-dynamic-rules [ verbose ] [ acsmgr instance` *`instance_number`* **`] [ | { grep`** *`grep_options`* **`| more } ]`**

acsmgr instance *instance_number*

Specifies the ACS/Session Manager instance ID as an integer from 1 through 65535.

verbose

Displays P2P Dynamic rule statistics in detail.

| { grep *grep_options* | more }

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

Usage Guidelines

Use this command to view P2P Dynamic signature file statistics/information.

Example

The following command displays P2P Dynamic rule information:

`show active-charging p2p-dynamic-rules`

show active-charging packet-filter

Displays information on packet filters configured in an Active Charging Service (ACS).

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show active-charging packet-filter { all | name` *`packet_filter_name`* **`} [ service name`** *`acs_service_name`* **`] [ | { grep`** *`grep_options`* **`| more } ]`**

all

Displays information for all packet filters configured, optionally all configured in an ACS.

name *packet_filter_name*

Displays detailed information for an existing packet filter specified as an alphanumeric string of 1 through 63 characters.

service name *acs_service_name*

Displays information for all filters or the specified packet filter in the specified ACS. *acs_service_name* must be the name of the ACS specified as an alphanumeric string of 1 through 15 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 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.

Usage Guidelines

Use this command to view information on packet filters configured in an ACS.

Example

The following command displays information for the packet filter *filter12*:

`show active-charging packet-filter name filter12`

show active-charging pcp-service

Displays statistics for Port Control Protocol (PCP) service in the Active Charging Service (ACS).

Important This command is customer specific. For more information contact your Cisco account representative.

Product

ACS

NAT

PSF

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

show active-charging pcp-service { all | name *pcp_service_name* **| statistics [instance** *instance_number* **| name** *pcp_service_name* **| wide] } [| { grep** *grep_options* **| more }]**

all

Displays information for all PCP services configured in the service.

name *pcp_service_name*

Displays information for an existing PCP service specified as an alphanumeric string of 1 through 63 characters.

statistics [instance *instance_number* | name *pcp_service_name* | wide]

Displays statistical information for all configured PCP services.

- **instance** *instance_number*: Displays statistics for the specified ACS/Session Manager instance.
- **name** *pcp_service_name*: Displays statistics for the specified PCP service.
- **wide**: Displays all available information in a single wide line.

| { grep *grep_options* | more }

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

Usage Guidelines

Use this command to view statistics for PCP service in the ACS.

show active-charging pcp-service statistics: The output of this command displays statistics for all PCP services in all contexts when issued in the local context. When issued in a specific context, this command displays statistics for all PCP services in that context.

show active-charging pcp-service instance *instance_number*: When issued in the local context, this command displays statistics for the specified ACS/Session Manager instance in all contexts. When issued in a specific context, this command displays statistics for the specified ACS/Session Manager instance in that context.

show active-charging pcp-service name *pcp_service_name*: The output of this command displays the statistics for the specified PCP service.

Example

The following command displays PCP service statistics for a PCP service named *pcp1*:

```
show active-charging pcp-service statistics name pcp1
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging qos-group-of-ruledefs

Displays information for ACS QoS-group-of-ruledefs.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show active-charging qos-group-of-ruledefs { all | name
qos_group_of_ruledefs_name } [ | { grep grep_options | more } ]
```

all

Displays details of all qos-group-of-ruledefs configured in the system.

name *qos_group_of_ruledefs_name*

Displays details for the specified qos-group-of-ruledefs.

qos_group_of_ruledefs_name must be the name of a qos-group-of-ruledefs, and must be 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 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.

Usage Guidelines

Use this command to view details of all/specific qos-group-of-ruledefs.

Example

The following command displays of a qos-group-of-ruledefs named *test*.

```
show active-charging qos-group-of-ruledefs name test
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging regex

Displays regular expression (regex) related statistics and information.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show active-charging regex { statistics { memory | ruledef } { all | instance` *`instance_number`* **`| summary } | status { all | instance`** *`instance_number`* **`} } [ | { grep`** *`grep_options`* **`| more } ]`**

statistics { memory | ruledef }{ all | instance *instance_number* | summary }

Displays regex-related statistics.

- **memory**: Displays regex memory related statistics.
- **ruledef**: Displays regex ruledef related statistics.
- **all**: Displays specified statistics for all Session Manager instances.
- **instance** *instance_number*: Displays specified statistics for specified Session Manager instance.

  instance_number must be an integer from 1 through 65535.
- **summary**: Displays summary information for specified parameter.

status { all | instance *instance_number* } }

Displays status information of regex engines.

- **all**: Displays status for all regex engines.
- **instance** *instance_number*: Displays status of regex engine for specified Session Manager instance.

  instance_number must be an integer from 1 through 65535.

| { grep *grep_options* | more }

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

Usage Guidelines

Use this command to view regular expression (regex) related statistics and status of regex engines.

Example

The following command displays status information of all regex engines:

```
show active-charging regex status all
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging rulebase

Displays information for ACS rulebases.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show active-charging rulebase { { { all | name rulebase_name } [ service name acs_service_name ] } | statistics [ name rulebase_name ] } [ | { grep grep_options | more } ]
```

all

Displays details of all rulebases configured in the system.

name *rulebase_name*

Displays details of an existing rulebase specified as an alphanumeric string of 1 through 63 characters.

service name *acs_service_name*

Displays details of all or the specified rulebase configured in the specified ACS. *acs_service_name* must be the name of the ACS, and must be an alphanumeric string of 1 through 15 characters.

statistics

Displays statistical information for all or the specified rulebase.

| { grep *grep_options* | more }

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

Usage Guidelines Use this command to view various statistics for a specific charging rulebase.

Example

The following command displays active charging rulebase statistics.

```
show active-charging rulebase statistics
```

The following command displays configurations and statistics for a rulebase named *rulebase_1*.

```
show active-charging rulebase name rulebase_1
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging ruledef

Displays information for ACS ruledefs.

Product ACS

PSF

Privilege Security Administrator, Administrator, Operator, Inspector

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show active-charging ruledef { all | charging | firewall | name ruledef_name
 | post-processing | routing | statistics [ all { charging | firewall [
wide ] | post-processing | tpo } | name ruledef_name [ wide ] ] | tpo } [ |
 { grep grep_options | more } ]
```

all

Displays information for all ruledefs configured in the ACS.

charging

Displays information for all Charging ruledefs configured in the ACS.

firewall

Displays information for all Stateful Firewall ruledefs configured in the ACS.

name *ruledef_name*

Displays detailed information for an existing ruledef specified as an alphanumeric string of 1 through 63 characters.

post-processing

Displays information for all post-processing ruledefs configured in the ACS.

routing

Displays information for all Routing ruledefs configured in the ACS.

service *service_name*

This keyword is obsolete.

statistics [all { charging | firewall [wide] | post-processing | tpo } | name *ruledef_name* [wide]]

Displays statistical information for all/specified ruledefs configured in the ACS. If none of the optional arguments are supplied, statistics totaled for all ruledefs will be displayed.

- **all**: Displays statistics for all ruledefs of the specified type configured in the ACS.
- **charging**: Displays statistics for all Charging ruledefs configured in the ACS.
- **firewall**: Displays statistics for all Firewall ruledefs configured in the service.
- **post-processing**: Displays statistics for all Post-processing ruledefs configured in the ACS.
- **tpo**

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

- **name** *ruledef_name*: Displays statistics for an existing ruledef specified as an alphanumeric string of 1 through 63 characters.
- **wide**: Displays all available information in a single wide line.

tpo

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

| { grep *grep_options* | more }

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

Usage Guidelines

Use this command to view information for ruledefs configured in the ACS.

Example

The following command displays ACS ruledef statistics.

```
show active-charging ruledef statistics
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging service

Displays detailed information about an Active Charging Service (ACS).

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show active-charging service { all | name *acs_service_name* **} [| { grep** *grep_options* **| more }]**

all

Displays information for all configured ACSs.

name *acs_service_name*

Displays detailed information for the ACS specified as an alphanumeric string of 1 through 15 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 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.

Usage Guidelines

Use this command to view ACS details.

Example

The following command displays details for the ACS named *test1*.

```
show active-charging service name test1
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging service-scheme

Displays statistics and information on active subscribers.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show active-charging service-scheme { all | name *serv_scheme_name* **| statistics [name** *serv_scheme_name* **] } [service name** *service_name* **] [| { grep** *grep_options* **| more }]**

all

Displays information for all service schemes configured in a service.

name *serv_scheme_name*

Displays detailed information for a specific service scheme.

serv_scheme_name must be an alphanumeric string of 1 through 63 characters.

statistics [name *serv_scheme_name*]

Displays the related statistics for the service-scheme.

name *serv_scheme_name* must be the name of a service-scheme and must be an alphanumeric string of 1 through 63 characters.

service *service_name*

Displays service and configuration counters for the specific active charging service.

service_name must be an alphanumeric string of 1 through 15 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 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.

Usage Guidelines Use this command to view subscriber statistics and information on dynamic updates to charging parameters per call ID.

Example

The following command displays all service-scheme statistics for the configured service-scheme *ss1*:

```
show active-charging service-scheme statistics name ss1
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging sessions

Displays statistics for Active Charging Service (ACS) sessions.

Product ACS

Privilege Security Administrator, Administrator, Operator, Inspector

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show active-charging sessions [ full [ wide ] | wf1 | summary ] [
filter_keyword + ] + [ all ] [ | { grep grep_options | more } ]
```

full [wide]

Displays all available information for the specified session.

Optionally all available information can be displayed in a single wide line.

summary

Displays active sessions count and packet and bytes statistics.

wf1

Displays all available information including MSISDN and rulebase in a single wide line.

display-dynamic-charging-rules

Displays information for the dynamic charging rules configured per session under Gx interface support.

dynamic-charging

Displays information for dynamic charging sessions.

filter_keyword

The following keywords are filters that modify or filter the output of the Command Keywords. Not all filters are available for all command keywords. Multiple filter keywords can be entered on a command line.

When multiple filter keywords are specified, the output conforms to all of the filter keywords specifications.

For example, if you enter the following command:

show active-charging sessions full active-charging-service acs_!

Counters for active charging sessions active in ACS *acs_1* with full details is displayed. Information for all other services is not displayed.

acsmgr instance *instance_number*

Displays session information for a specific ACS/Session Manager instance.

active-charging-service *acs_service_name*

Displays session information for the ACS specified as an alphanumeric string of 1 through 15 characters.

all

Displays session information for all active charging sessions.

cae-readdressing

Displays the Content Adaptation Engine (CAE) re-addressing session information for active charging sessions.

callid

Specifies the call identification number.

display-dynamic-charging-rules

Displays dynamic charging rules configured.

dynamic-charging

Displays session information for all dynamic charging sessions.

firewall { not-required | required }

Displays session information for sessions with Firewall Processing required or not required, as specified.

flows {active | idle | total} [< | = | > | equal-to | greater-than | less-than] { *bytes* }

Displays information for all active charging flows filtered by all information, active, or idle sessions.

- < *bytes*or **less-than** *bytes*: Specifies filtering of flows that is less than the specified number of bytes.
- > *bytes*or **greater-than** *bytes*: Specifies filtering of flows that is greater than the specified number of bytes.
- = *bytes*or **equal-to** *bytes*: Specifies filtering of flows that is equal to the specified number of bytes.

bytes must be an integer from 0 through 18446744073709551615.

fw-and-nat policy *fw_nat_policy_name*

Displays information for the Firewall-and-NAT Policy specified as an alphanumeric string of 1 through 63 characters.

imsi

Specifies the International Mobile Subscriber Identity (IMSI) of the subscriber session.

ip-address

Specifies the IP address for the specific charging service.

max-flows { < | = | > | equal-to | greater-than | less-than }{ *bytes* }

Displays information for the maximum flows made by the session.

- < *bytes*or **less-than** *bytes*: Specifies filtering of maximum flows that is less than the specified number of bytes.
- > *bytes*or **greater-than** *bytes*: Specifies filtering of maximum flows that is greater than the specified number of bytes.
- = *bytes*or **equal-to** *bytes*: Specifies filtering of maximum flows that is equal to the specified number of bytes.

bytes must be an integer from 0 through 18446744073709551615.

msid

Displays active charging session information for a specific subscriber's Mobile Station Identification (MSID) number.

msisdn *msisdn_number*

Displays active charging session information for a specific subscriber's Mobile Station Integrated Services Digital Network (MSISDN) number.

msisdn_number must be an integer with a maximum of 15 digits.

ipv4

Displays active charging session information with IPv4 Firewall enabled/disabled.

ipv6

Displays active charging session information with IPv6 Firewall enabled/disabled.

nat { not-required | required [nat-realm *nat_realm_name*] } [ipv4 | ipv6]

Displays session information for sessions with NAT required or not required, as specified.

nat-realm *nat_realm_name* specifies the name of a NAT realm as an alphanumeric string of 1 through 63 characters.

ipv4: Displays active-charging sessions for which NAT44 processing is required.

ipv6: Displays active-charging sessions for which NAT64 processing is required.

rulebase

Displays information for a rulebase that is configured in an active charging session.

rx-data

Displays the bytes received in the session.

session-id

Displays detailed session information for a specific session identification.

transrating

Displays the transrating sessions.

tx-data

Displays the bytes sent in the session.

type

Displays session information for specified DNS application type(s).

- **dns**
- **ftp**
- **h323**
- **http**
- **icmp**
- **icmpv6**
- **imap**
- **ip**
- **ipv6**
- **mms**
- **p2p [application** *p2p_list* **[traffic-type** *traffic_type* **] | protocol-group** *group_list* **]**: Displays session information for a P2P application type and P2P protocol group.

  p2p application *p2p_list*: The supported P2P applications are:

  - **8tracks**
  - **abcnetworks**
  - **actionvoip**
  - **actsync**

- **adobeconnect**
- **aimini**
- **amazoncloud**
- **amazonmusic**
- **amazonvideo**
- **antsp2p**
- **apple-push**
- **apple-store**
- **applejuice**
- **applemaps**
- **ares**
- **armagettron**
- **avi**
- **badoo**
- **baidumovie**
- **battlefld**
- **bbm**
- **beatport**
- **betternet**
- **bitcasa**
- **bittorrent**
- **bittorrent-sync**
- **blackberry-store**
- **blackberry**
- **blackdialer**
- **box**
- **callofduty**
- **chikka**
- **cisco-jabber**
- **citrix**
- **clubbox**
- **clubpenguin**

- **crackle**
- **crossfire**
- **crunchyroll**
- **cyberghost**
- **ddlink**
- **deezer**
- **didi**
- **directconnect**
- **dish-anywhere**
- **disneymovies**
- **dofus**
- **dramafever**
- **dropbox**
- **edonkey**
- **espn**
- **expressvpn**
- **facebook**
- **facetime**
- **fandor**
- **fasttrack**
- **feidian**
- **fiesta**
- **filetopia**
- **filmontv**
- **flash**
- **flickr**
- **florensia**
- **foursquare**
- **fox-sports**
- **freenet**
- **friendster**
- **fring**

- **funshion**
- **gadu_gadu**
- **gamekit**
- **gmail**
- **gnutella**
- **go90**
- **goober**
- **google-music**
- **google-push**
- **google**
- **googleplay**
- **googleplus**
- **gotomeeting**
- **gtalk**
- **guildwars**
- **halflife2**
- **hamachivpn**
- **hayu**
- **hbogo**
- **hbonow**
- **heytell**
- **hgtv**
- **hike-messenger**
- **hls**
- **hotspotvpn**
- **hulu**
- **hyves**
- **iax**
- **icall**
- **icecast**
- **icloud**
- **idrive**

- **igo**
- **iheartradio**
- **imesh**
- **imessage**
- **imgur**
- **imo**
- **instagram**
- **iplayer**
- **iptv**
- **irc**
- **isakmp**
- **iskoot**
- **itunes**
- **jabber**
- **jap**
- **jumblo**
- **kakaotalk**
- **kik-messenger**
- **kontiki**
- **kugoo**
- **kuro**
- **linkedin**
- **livestream**
- **lync**
- **magicjack**
- **manolito**
- **mapfactor**
- **mapi**
- **maplestory**
- **meebo**
- **mgcp**
- **mlb**

- **mojo**
- **monkey3**
- **mozy**
- **msn**
- **msrp**
- **mute**
- **mypeople**
- **myspace**
- **nateontalk**
- **naverline**
- **navigon**
- **nbc-sports**
- **netmotion**
- **newsy**
- **nick**
- **nimbuzz**
- **nokia-store**
- **octoshape**
- **off**
- **ogg**
- **oist**
- **oovoo**
- **opendrive**
- **openft**
- **openvpn**
- **orb**
- **oscar**
- **outlook**
- **paltalk**
- **pando**
- **pandora**
- **path**

- **pbs**
- **pcanywhere**
- **periscope**
- **pinterest**
- **plingm**
- **poco**
- **popo**
- **pplive**
- **ppstream**
- **ps3**
- **qq**
- **qqgame**
- **qqlive**
- **quake**
- **quic**
- **quicktime**
- **radio-paradise**
- **radius**
- **rdp**
- **rdt**
- **regram**
- **rfactor**
- **rhapsody**
- **rmstream**
- **rodi**
- **rynga**
- **samsung-store**
- **scydo**
- **secondlife**
- **shoutcast**
- **showtime**
- **silverlight**

- **siri**
- **skinny**
- **skydrive**
- **skype**
- **slacker-radio**
- **slingbox**
- **slingtv**
- **smartvoip**
- **snapchat**
- **softether**
- **sopcast**
- **soribada**
- **soulseek**
- **soundcloud**
- **spark**
- **spdy**
- **speedtest**
- **spike**
- **splashfighter**
- **spotify**
- **ssdp**
- **starz**
- **stealthnet**
- **steam**
- **stun**
- **sudaphone**
- **svtplay**
- **tagged**
- **talkatone**
- **tango**
- **teamspeak**
- **teamviewer**

- **telegram**
- **thunder**
- **tinder**
- **tmo-tv**
- **tor**
- **truecaller**
- **truphone**
- **tumblr**
- **tunein-radio**
- **tunnelvoice**
- **turbovpn**
- **tvants**
- **tvland**
- **tvuplayer**
- **twitch**
- **twitter**
- **ultrabac**
- **ultrasurf**
- **univision**
- **upc-phone**
- **usenet**
- **ustream**
- **uusee**
- **vchat**
- **veohtv**
- **vessel**
- **vevo**
- **viber**
- **vine**
- **voipdiscount**
- **vopium**
- **vpnmaster**

- **vpnx**
- **voxer**
- **vtok**
- **vtun**
- **vudu**
- **warcft3**
- **waze**
- **webex**
- **wechat**
- **whatsapp**
- **wii**
- **windows-azure**
- **windows-store**
- **winmx**
- **winny**
- **wmstream**
- **wofkungfu**
- **wofwarcraft**
- **wuala**
- **xbox**
- **xdcc**
- **xing**
- **yahoo**
- **yahoomail**
- **yiptv**
- **youku**
- **yourfreetunnel**
- **youtube**
- **zattoo**

traffic-type *traffic_type*: P2P protocol flows include the following traffic type classifications:

Important The traffic type for a P2P protocol may vary depending on the P2P protocol.

- **ads**
- **audio**
- **file-transfer**
- **im**
- **video**
- **voipout**
- **unclassified**

p2p protocol-group *group_list*: The following P2P protocol groups are supported:

- generic
- anonymous-access
- business
- communicator
- cloud
- e-store
- e-mail
- e-news
- internet-privacy
- filesharing
- gaming
- p2p-filesharing
- p2p-anon-filesharing
- remote-control
- social-nw-gaming
- social-nw-generic
- social-nw-videoconf
- standard
- streaming

- **pop3**
- **pptp**
- **rtcp**
- **rtp**
- **rtsp**
- **secure-http**
- **sip**

- **smtp**
- **tcp**
- **tftp**
- **udp**
- **unknown**
- **wsp-connection-less**
- **wsp-connection-oriented**

username

Displays session information for a specific user name.

dynamic-charging

Displays all the sessions having received at least one Gx message from Session Manager/IMS Authorization.

| { grep *grep_options* | more }

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

Usage Guidelines

Use this command to display the configuration information for an active charging session.

Example

The following command displays full information of an active charging session.

```
show active-charging sessions full all
```

The following command displays an active charging session summary.

```
show active-charging sessions summary
```

Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging sessions credit-control server-unreachable

Displays the details of sessions that are currently in server-unreachable state i.e. Gy Assume Positive state.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

show active-charging sessions credit-control server-unreachable [*filter_keyword* **+] [| { grep** *grep_options* **| more }]**

filter_keyword

The following keywords are filters that modify or filter the output of the Command Keywords. Not all filters are available for all command keywords. Multiple filter keywords can be entered on a command line.

When multiple filter keywords are specified, the output conforms to all of the filter keywords specifications.

For example, if you enter the following command:

show active-charging sessions credit-control server-unreachable active-charging-service acs_1

Counters for active charging sessions active in ACS *acs_1* are displayed. Information for all other services is not displayed.

acsmgr *instance_number*

Displays session information for a specific ACS/Session Manager instance.

active-charging-service *acs_service_name*

Displays session information for the ACS specified as an alphanumeric string of 1 through 15 characters.

callid

Specifies the call identification number.

credit-control

Displays credit control information.

dynamic-charging

Displays session information for all dynamic charging sessions.

firewall { not-required | required }

Displays session information for sessions with Firewall Processing required or not required, as specified.

flows {active | idle | total} [< | = | > | equal-to | greater-than | less-than] { *bytes* }

Displays information for all active charging flows filtered by all information, active, or idle sessions.

- < *bytes*or **less-than** *bytes*: Specifies filtering of flows that is less than the specified number of bytes.
- > *bytes*or **greater-than** *bytes*: Specifies filtering of flows that is greater than the specified number of bytes.

- **=** *bytes*or **equal-to** *bytes*: Specifies filtering of flows that is equal to the specified number of bytes.

bytes must be an integer from 0 through 18446744073709551615.

fw-and-nat policy *fw_nat_policy_name*

Displays information for the Firewall-and-NAT Policy specified as an alphanumeric string of 1 through 63 characters.

imsi

Specifies the International Mobile Subscriber Identity (IMSI) of the subscriber session.

ip-address

Specifies the IP address for the specific charging service.

max-flows { < | = | > | equal-to | greater-than | less-than }{ *bytes* }

Displays information for the maximum flows made by the session.

- **<** *bytes*or **less-than** *bytes*: Specifies filtering of maximum flows that is less than the specified number of bytes.
- **>** *bytes*or **greater-than** *bytes*: Specifies filtering of maximum flows that is greater than the specified number of bytes.
- **=** *bytes*or **equal-to** *bytes*: Specifies filtering of maximum flows that is equal to the specified number of bytes.

bytes must be an integer from 0 through 18446744073709551615.

msid

Displays active charging session information for a specific subscriber's Mobile Station Identification (MSID) number.

rulebase

Displays information for a rulebase that is configured in an active charging session.

rx-data

Displays the bytes received in the session.

session-id

Displays detailed session information for a specific session identification.

tx-data

Displays the bytes sent in the session.

type

Displays session information for specified DNS application type(s).

- **dns**
- **ftp**
- **h323**
- **http**
- **icmp**
- **icmpv6**
- **imap**
- **ip**
- **ipv6**
- **mms**
- **p2p [application** *p2p_list* **[traffic-type** *traffic_type* **] | protocol-group** *group_list* **]**: Displays session information for a P2P application type and P2P protocol group.

  p2p application *p2p_list*: The supported P2P applications are:

  - **8tracks**
  - **abcnetworks**
  - **actionvoip**
  - **actsync**
  - **adobeconnect**
  - **aimini**
  - **amazoncloud**
  - **amazonmusic**
  - **amazonvideo**
  - **antsp2p**
  - **apple-push**
  - **apple-store**
  - **applejuice**
  - **applemaps**
  - **ares**
  - **armagettron**
  - **avi**

- **badoo**
- **baidumovie**
- **battlefld**
- **bbm**
- **beatport**
- **betternet**
- **bitcasa**
- **bittorrent**
- **bittorrent-sync**
- **blackberry-store**
- **blackberry**
- **blackdialer**
- **box**
- **callofduty**
- **chikka**
- **cisco-jabber**
- **citrix**
- **clubbox**
- **clubpenguin**
- **crackle**
- **crossfire**
- **crunchyroll**
- **cyberghost**
- **ddlink**
- **deezer**
- **didi**
- **directconnect**
- **dish-anywhere**
- **disneymovies**
- **dofus**
- **dramafever**
- **dropbox**

- **edonkey**
- **espn**
- **expressvpn**
- **facebook**
- **facetime**
- **fandor**
- **fasttrack**
- **feidian**
- **fiesta**
- **filetopia**
- **filmontv**
- **flash**
- **flickr**
- **florensia**
- **foursquare**
- **fox-sports**
- **freenet**
- **friendster**
- **fring**
- **funshion**
- **gadu_gadu**
- **gamekit**
- **gmail**
- **gnutella**
- **go90**
- **goober**
- **google-music**
- **google-push**
- **google**
- **googleplay**
- **googleplus**
- **gotomeeting**

- **gtalk**
- **guildwars**
- **halflife2**
- **hamachivpn**
- **hayu**
- **hbogo**
- **hbonow**
- **heytell**
- **hgtv**
- **hike-messenger**
- **hls**
- **hotspotvpn**
- **hulu**
- **hyves**
- **iax**
- **icall**
- **icecast**
- **icloud**
- **idrive**
- **igo**
- **iheartradio**
- **imesh**
- **imessage**
- **imgur**
- **imo**
- **instagram**
- **iplayer**
- **iptv**
- **irc**
- **isakmp**
- **iskoot**
- **itunes**

- **jabber**
- **jap**
- **jumblo**
- **kakaotalk**
- **kik-messenger**
- **kontiki**
- **kugoo**
- **kuro**
- **linkedin**
- **livestream**
- **lync**
- **magicjack**
- **manolito**
- **mapfactor**
- **mapi**
- **maplestory**
- **meebo**
- **mgcp**
- **mlb**
- **mojo**
- **monkey3**
- **mozy**
- **msn**
- **msrp**
- **mute**
- **mypeople**
- **myspace**
- **nateontalk**
- **naverline**
- **navigon**
- **nbc-sports**
- **netmotion**

- **newsy**
- **nick**
- **nimbuzz**
- **nokia-store**
- **octoshape**
- **off**
- **ogg**
- **oist**
- **oovoo**
- **opendrive**
- **openft**
- **openvpn**
- **orb**
- **oscar**
- **outlook**
- **paltalk**
- **pando**
- **pandora**
- **path**
- **pbs**
- **pcanywhere**
- **periscope**
- **pinterest**
- **plingm**
- **poco**
- **popo**
- **pplive**
- **ppstream**
- **ps3**
- **qq**
- **qqgame**
- **qqlive**

- **quake**
- **quic**
- **quicktime**
- **radio-paradise**
- **radius**
- **rdp**
- **rdt**
- **regram**
- **rfactor**
- **rhapsody**
- **rmstream**
- **rodi**
- **rynga**
- **samsung-store**
- **scydo**
- **secondlife**
- **shoutcast**
- **showtime**
- **silverlight**
- **siri**
- **skinny**
- **skydrive**
- **skype**
- **slacker-radio**
- **slingbox**
- **slingtv**
- **smartvoip**
- **snapchat**
- **softether**
- **sopcast**
- **soribada**
- **soulseek**

- **soundcloud**
- **spark**
- **spdy**
- **speedtest**
- **spike**
- **splashfighter**
- **spotify**
- **ssdp**
- **starz**
- **stealthnet**
- **steam**
- **stun**
- **sudaphone**
- **svtplay**
- **tagged**
- **talkatone**
- **tango**
- **teamspeak**
- **teamviewer**
- **telegram**
- **thunder**
- **tinder**
- **tmo-tv**
- **tor**
- **truecaller**
- **truphone**
- **tumblr**
- **tunein-radio**
- **tunnelvoice**
- **turbovpn**
- **tvants**
- **tvland**

- **tvuplayer**
- **twitch**
- **twitter**
- **ultrabac**
- **ultrasurf**
- **univision**
- **upc-phone**
- **usenet**
- **ustream**
- **uusee**
- **vchat**
- **veohtv**
- **vessel**
- **vevo**
- **viber**
- **vine**
- **voipdiscount**
- **vopium**
- **vpnmaster**
- **vpnx**
- **voxer**
- **vtok**
- **vtun**
- **vudu**
- **warcft3**
- **waze**
- **webex**
- **wechat**
- **whatsapp**
- **wii**
- **windows-azure**
- **windows-store**

- **winmx**
- **winny**
- **wmstream**
- **wofkungfu**
- **wofwarcraft**
- **wuala**
- **xbox**
- **xdcc**
- **xing**
- **yahoo**
- **yahoomail**
- **yiptv**
- **youku**
- **yourfreetunnel**
- **youtube**
- **zattoo**

traffic-type *traffic_type*: P2P protocol flows include the following traffic type classifications:

Important The traffic type for a P2P protocol may vary depending on the P2P protocol.

- **ads**
- **audio**
- **file-transfer**
- **im**
- **video**
- **voipout**
- **unclassified**

p2p protocol-group *group_list*: The following P2P protocol groups are supported:

- generic
- anonymous-access
- business
- communicator

- cloud
- e-store
- e-mail
- e-news
- internet-privacy
- filesharing
- gaming
- p2p-filesharing
- p2p-anon-filesharing
- remote-control
- social-nw-gaming
- social-nw-generic
- social-nw-videoconf
- standard
- streaming

- **pop3**
- **pptp**
- **rtcp**
- **rtp**
- **rtsp**
- **secure-http**
- **sip**
- **smtp**
- **tcp**
- **tftp**
- **udp**
- **unknown**
- **wsp-connection-less**
- **wsp-connection-oriented**

username

Displays session information for a specific user name.

| { grep *grep_options* | more }

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

Usage Guidelines Use this command to display the configuration information for an active charging session.

Example

The following command displays full information of an active charging session.

```
show active-charging sessions full all
```

The following command displays an active charging session summary.

```
show active-charging sessions summary
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging subscribers

Displays statistics and information on active subscribers.

Product ACS

Privilege Security Administrator, Administrator, Operator, Inspector

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show active-charging subscribers callid call_id charging-updates [ statistics ] [ charging-action [ name charging_action_name ] | qos-group [ name qos_group_of_ruledefs_name ] | session ] [ | { grep grep_options | more } ]
```

callid *call_id*

Specifies a call identification number.

call_id must be an eight digit HEX number.

charging-updates [statistics] [charging-action [name *charging_action_name*] | qos-group [name *qos_group_of_ruledefs_name*] | session]

Displays charging-update statistics for subscriber.

- **statistics**: Displays statistics related to dynamic updates to charging parameters.
- **charging-action [name** *charging_action_name* **]**: Displays charging-updates for activated charging-actions or specified charging action.

  charging_action_name must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters in length.

- **qos-group [name** *qos_group_of_ruledefs_name* **]**: Displays charging-updates for activated QoS groups or the specified QoS-group-of-ruledefs.

  qos_group_of_ruledefs_name must be the name of a QoS-group-of-ruledefs, and must be an alphanumeric string of 1 through 63 characters in length.

- **session**: Displays charging-updates for the session.

| { grep *grep_options* | more }

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

Usage Guidelines

Use this command to view subscriber statistics and information on dynamic updates to charging parameters per call ID.

Example

The following command displays all statistics related to dynamic updates to charging parameters for call ID *ca50ea54*:

```
show active-charging subscribers callid ca50ea54 charging-updates
statistics
```

The following command displays information on charging updates for call ID *ca50ea54* and ACS charging action named *test12*:

```
show active-charging subscribers callid ca50ea54 charging-updates
charging-action name test12
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging subsystem

Displays service and configuration counters for the ACS.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show active-charging subsystem { all | facility acsmgr { all | instance *instance_number* **} [rulebase name** *rulebase_name* **] | sip } [| { grep** *grep_options* **| more }]**

all

Displays ACS subsystem information.

facility acsmgr [all | instance *instance_number*]

Displays logged events for all ACS/Session Managers or for a specific instance.

instance_number must be an integer from 1 through 65535.

rulebase name *rulebase_name*

Displays rulebase statistics for the specified rulebase.

rulebase_name must be the name of a rulebase, and must be an alphanumeric string of 1 through 63 characters.

sip

Displays SIP related statistics.

| { grep *grep_options* | more }

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

Usage Guidelines

Use this command to view ACS/Session Manager information.

Example

The following command displays ACS subsystem information:

```
show active-charging subsystem all
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging tcp-proxy statistics

Displays TCP Proxy statistics.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

show active-charging tcp-proxy statistics [all | dynamic-disable | ip-layer | proxy-fac | rulebase *rulebase_name* **| socket-migration | tcp-layer] [verbose] [| { grep** *grep_options* **| more }]**

all

Displays all TCP Proxy statistics aggregated over all rulebases, including for both IP and TCP layers.

dynamic-disable

Displays statistics for dynamic disabling of TCP Proxy.

ip-layer

Displays TCP Proxy statistics for IP layer.

proxy-fac

Displays TCP Proxy Flow Admission Control statistics.

rulebase *rulebase_name*

Displays TCP Proxy statistics for the rulebase specified as an alphanumeric string of 1 through 63 characters.

socket-migration

Displays TCP Proxy statistics for socket migration.

tcp-layer

Displays TCP Proxy statistics for TCP layer.

verbose

Displays detailed TCP Proxy statistics.

| { grep *grep_options* | more }

Specifies that the output of this command is to be piped (sent) to the command specified. You must specify a command to which the output 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.

Usage Guidelines

Use this command to view TCP Proxy statistics.

Example

The following command displays detailed TCP proxy statistics for the rulebase named *test14*:

```
show active-charging tcp-proxy statistics rulebase test14 verbose
```

show active-charging tethering-detection

Displays information/statistics pertaining to Tethering Detection databases.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

show active-charging tethering-detection { database [os-signature | tac | ua-signature]+ [sessmgr { all | instance *instance_number* **}] [| { grep** *grep_options* **| more }] | statistics }**

database [os-signature | tac | ua-signature]+ [sessmgr { all | instance *instance_number* }]

Displays information pertaining to the specified Tethering Detection database(s).

- **os-signature**: Displays Tethering Detection OS (Operating System) database information.
- **tac**: Displays Tethering Detection TAC (Transaction Authorization Code) database information.
- **ua-signature**: Displays Tethering Detection UA (User Agent) database information.
- **+**: Indicates that more than one of the preceding keywords can be entered in a single command.
- **sessmgr { all | instance** *instance_number* **}**: Displays SessMgr Tethering Detection database status.
  - **all**: Displays status for all SessMgr instances.
  - **instance** *instance_number*: Displays status for the SessMgr instance specified as an integer from 1 through 10000.

statistics

Displays Tethering Detection related statistics.

| { grep *grep_options* | more }

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

Usage Guidelines

Use this command to view information/statistics pertaining to Tethering Detection databases.

Example

The following command displays information pertaining to Tethering Detection UA and OS databases:

show active-charging tethering-detection database ua-signature os-signature

The following command displays information pertaining to all Tethering Detection databases:

show active-charging tethering-detection database

show active-charging timedef

Displays the details of timeslots configured in specified time definition(s).

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

show active-charging timedef { all | name *timedef_name* **} [service name** *acs_service_name* **] [| { grep** *grep_options* **| more }]**

all

Displays information for all timedefs configured in the service.

name *timedef_name*

Displays detailed information for the timedef specified s an alphanumeric string of 1 through 63 characters.

service name *acs_service_name*

Displays information for all or a specific timedef configured in the specified ACS. *acs_service_name* must be the name of the active-charging service, and must be an alphanumeric string of 1 through 15 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 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.

Usage Guidelines

Use this command to view details of timeslots configured in specified timedef(s) that have been configured for the Time-of-Day Activation/Deactivation of Rules feature.

Example

The following command displays timeslot details of all timedefs configured in the ACS:

show active-charging timedef all

show active-charging traffic-optimization counters sessmgr

Displays cumulative Traffic Optimization statistics from Cisco Ultra Traffic Optimization engine.

Important This command is license dependent. For more information, contact your Cisco account representative.

Product

P-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

show active-charging traffic-optimization counters sessmgr { all | instance *number* **}**

counters

Displays aggregate flow counters/statistics from Cisco Ultra Traffic Optimization engine.

all

Displays all session manager (sessmgr) statistics specific to Traffic Optimization.

instance *number*

Displays the statistics for a session manager instance.

Usage Guidelines

Use this command to display cumulative Traffic Optimization statistics from Cisco Ultra Traffic Optimization engine.

Example

The following command displays all sessmgr Traffic Optimization statistics from Cisco Ultra Traffic Optimization engine:

show active-charging traffic-optimization counters sessmgr all

show active-charging traffic-optimization info

Displays version, mode, and configuration values of Cisco Ultra Traffic Optimization engine.

Product

P-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show active-charging traffic-optimization info`

traffic-optimization

Displays all Traffic Optimization options.

info

Displays Cisco Ultra Traffic Optimization engine information.

Usage Guidelines

Use this command to display version, mode, and configuration values of Cisco Ultra Traffic Optimization engine. The output of configured values is based on Cisco Ultra Traffic Optimization engine. Only the relevant information for each Cisco Ultra Traffic Optimization engine is displayed as part of this CLI output.

Example

The following command displays detailed statistics about the version, mode, and configuration values of Cisco Ultra Traffic Optimization engine:

`show active-charging traffic-optimization info`

show active-charging trigger-action

Displays information about the trigger actions configured in a service.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show active-charging trigger-action { all | name` *`trigger_action_name`* **`[ service`** *`acs_service_name`* **`] } [ | { grep`** *`grep_options`* **`| more } ]`**

all

Displays information for all trigger actions configured in a service.

name *trigger_action_name*

Displays information for the specified trigger action.

trigger_action_name must be specified as an alphanumeric string of 1 through 63 characters.

service *acs_service_name*

Displays service and configuration counters for the specified active charging service.

acs_service_name must be specified 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 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.

Usage Guidelines

Use this command to view information about trigger actions configured in a service.

Example

The following command displays the information for all trigger actions:

```
show active-charging trigger-action all
```

Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging trigger-condition

Displays information about the trigger conditions configured in a service.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show active-charging trigger-condition { { all | name trigger_condn_name [
service acs_service_name ] } | statistics [ name trigger_condn_name ] } [ | {
grep grep_options | more } ]
```

all

Displays information for all trigger conditions configured in a service.

name *trigger_condn_name*

Displays information for the specified trigger condition.

trigger_condn_name must be specified as an alphanumeric string of 1 through 63 characters.

statistics

Displays statistical information for all configured trigger conditions.

service *acs_service_name*

Displays service and configuration counters for the specified active charging service.

acs_service_name must be specified 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 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.

Usage Guidelines

Use this command to view information about trigger conditions configured in a service.

Example

The following command displays the information for all trigger conditions:

```
show active-charging trigger-condition all
```

Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging udr-format

Displays information about UDR formats configured in an Active charging Service (ACS).

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show active-charging udr-format { all | name *udr_fromat_name* **} [| { grep** *grep_options* **| more }]**

all

Displays information for all UDR formats.

name *udr_fromat_name*

Displays information for an existing UDR format specified 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 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.

Usage Guidelines

Use this command to display information for UDR format(s) in an ACS.

Example

The following command displays all configured UDR formats in an ACS.

show active-charging udr-format all

Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging url-blockedlisting statistics

Displays URL Blockedlisting statistics.

Product

CF

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

In releases prior to StarOS 21.26:

show active-charging url-blacklisting statistics [rulebase { all | name *rulebase_name* **}] [verbose] [| { grep** *grep_options* **| more }]**

From StarOS 21.26 and later releases:

show active-charging url-blockedlisting statistics [rulebase { all | name *rulebase_name* **}] [verbose] [| { grep** *grep_options* **| more }]**

rulebase { all | name *rulebase_name* }

Displays URL Blockedlisting statistics for all or a specific rulebase.

- **all**: Displays URL Blockedlisting statistics for all configured rulebases.
- **name** *rulebase_name*: Displays URL Blockedlisting statistics for the rulebase specified as an alphanumeric string of 1 through 63 characters.

verbose

Displays detailed URL Blockedlisting statistics.

| { grep *grep_options* | more }

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

Usage Guidelines

Use this command to view URL Blockedlisting hits and misses statistics.

Example

In releases prior to StarOS 21.26:

The following command displays cumulative URL Blacklisting statistics:

show active-charging url-blacklisting statistics

The following command displays URL Blacklisting statistics for the rulebase *rulebase_1*:

show active-charging url-blacklisting statistics rulebase name rulebase_1

From StarOS 21.26 and later releases:

The following command displays cumulative URL Blockedlisting statistics:

show active-charging url-blockedlisting statistics

The following command displays URL Blockedlisting statistics for the rulebase *rulebase_1*:

show active-charging url-blockedlisting statistics rulebase name rulebase_1

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging video detailed-statistics

Displays detailed statistics for TCP video flows. The command options enable you to collect statistical data for video per UE device type, per radio access type, and per video container type.

Important In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

Product

MVG

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

```
show active-charging video detailed-statistics [ container { flv | mp4 |
 others } | rat { cdma | gprs | hspa | lte | others | umts | wlan } | ue
 { android | ios | laptop | others } ]
```

container { flv | mp4 | others }

Displays detailed statistics for TCP video flows based on the specified container file format.

rat { cdma | gprs | hspa | lte | others | umts | wlan }

Displays detailed statistics for TCP video flows based on the specified radio access type.

ue { android | ios | laptop | others }

Displays detailed statistics for TCP video flows based on the specified UE device type.

Usage Guidelines

Use this command to display detailed statistics about video usage. Use the command options to display detailed statistics based on the UE device type, radio access type, or container file format.

Example

The following command displays detailed statistics about video usage based on the UE device type *ios*:

```
show active-charging video detailed-statistics ue ios
```

show active-charging xheader-format

Displays x-header format configurations for an Active Charging Service (ACS).

Important This is a customer-specific command. Please contact your local sales representative for more information.

Product ACS

Privilege Security Administrator, Administrator, Operator, Inspector

Command Modes Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description **`show active-charging xheader-format { all | name`** *`xheader_format`* **`} [ | { grep`** *`grep_options`* **`| more } ]`**

all

Displays information for all x-header formats configured.

name *xheader_format*

Displays information for the x-header format specified 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 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.

Usage Guidelines Use this command to view details of x-header formats configured in an ACS.

Example

The following command displays information for the x-header format named *test12*:

```
show active-charging xheader-format test12
```

show administrators

Displays information regarding all CLI users currently connected to the system.

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 **show administrators [session id] [| { grep** *grep_options* **| more }]**

session id

Indicates the output is to contain additional information about the CLI user session including the assigned session ID.

| { 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.

Usage Guidelines This command displays a list of administrative users that have command line interface sessions active.

Example

The following command displays a list of administrative users with active command line interface sessions:

```
show administrators
```

The following command displays the list along with CLI user session IDs:

```
show administrators session id
```

show alarm

Displays alarm information.

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 **show alarm { all | audible | central-office | facility | outstanding [all | chassis | port** *slot/port* **| slot** *slot* **] [verbose] | statistics } [| { grep** *grep_options* **| more }]**

all

Displays the state of all alarms in one screen.

audible

Displays the state of the internal audible alarm on the SMC (ASR 5000) or SSC (ASR 5500).

central-office

Displays the state of the CO Alarm contacts on the SPIO (ASR 5000) or SSC (ASR 5500).

facility

Displays the state of the facility (audible and CO) alarms.

outstanding [all | chassis | port *slot/port* | slot *slot*] [verbose]

Displays information on currently outstanding alarms.

- **all**: Displays all alarm information.
- **chassis**: Displays chassis/power/fan alarms.
- **port** *slot/port*: Shows the alarm information for the specified port.
- **slot** *slot*: Shows the alarm information for the card in the specified slot.
- **verbose**: Displays more verbose output, including the internal alarm ID

statistics

Displays basic statistics on the alarming subsystem, including the current number of outstanding alarms of different severities and a cumulative total of alarms generated.

| { 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 Output* section of the *Command Line Interface Overview* chapter.

Usage Guidelines

View alarms to verify system status or to periodically check the general health of the system.

Important This command is not supported on all platforms.

Example

The following command displays all alarms that are currently outstanding:

```
show alarm outstanding all
```

The following command displays more detailed information on all alarms that are currently outstanding:

```
show alarm outstanding all verbose
```

The following command displays alarm statistics:

```
show alarm statistics
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show alcap counters

Important In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Displays the Access Link Control Application Part (ALCAP) protocol message counters related to ALCAP protocol sessions associated with a Home-NodeB Gateway (HNB-GW) service instance configured and running on a system.

Product

HNBGW

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show alcap counters [alcap-service *alcap_svc_name* **[aal2-node** *aal2_node_name* **[aal2-path** *aal2_path_id* **]]] [| { grep** *grep_options* **| more }]**

name *alcap_svc_name*

Specifies the name of the ALCAP service for which ALCAP protocol session counters are to be displayed.

aal2-node *aal2-node*

Specifies the name of the ATM Adaptation Layer 2 (AAL2) node for which protocol session counters will be filtered.

aal2-path *aal2_path_id*

Specifies the identity number of the AAL2 path on a specific ATM Adaptation Layer 2 (AAL2) node for which ALCAP protocol counters will be filtered.

| { 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 the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in *Command Line Interface Overview* chapter.

Usage Guidelines

This command is used to display the sessions statistics and counters for ALCAP service.

Example

The following command displays the ALCAP protocol session counters for ALCAP service named as *alcap_hnb_svc1*:

```
show alcap counters alcap-service alcap_hnb_svc1
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show alcap-service

Important In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Displays the Access Link Control Application Part (ALCAP) session statistics of an ALCAP service associated with a Home-NodeB Gateway (HNB-GW) service instance configured and running on a system.

Product

HNBGW

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show alcap-service { all | name *alcap_svc_name* **[aal2-node** *aal2_node_name* **[aal2-path** *aal2_path_id* **[aal2-channel** *aal2_channel_num*]] **| endpoint** *aal2_endpoint_name* **] } [| { grep** *grep_options* **| more }]**

name *alcap_svc_name*

Specifies the name of the ALCAP service for which service statistics are to be displayed.

aal2-node *aal2-node*

Specifies the name of the ATM Adaptation Layer 2 (AAL2) node that will be used to filter the display of the ALCAP service statistics.

aal2-path *aal2_path_id*

Specifies the identity number of the AAL2 path on a specific ATM Adaptation Layer 2 (AAL2) node that will be used to filter the display of the ALCAP service statistics.

aal2-channel *aal2_channel_num*

Specifies the AAL2 channel number of the AAL2 path on a specific ATM Adaptation Layer 2 (AAL2) node that will be used to filter the display of the ALCAP service statistics.

endpoint *atm_endpoint_name*

Specifies the ATM endpoint name that will be used to filter the display of the ALCAP service statistics for a specific ATM endpoint.

Usage Guidelines

This command is used to clear the sessions statistics and counters for ALCAP service.

Example

The following command displays the service statistics of ALCAP service named as *alcap_hnb_svc1*:

```
show alcap-service name alcap_hnb_svc1
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show alcap statistics

Important In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Displays the session statistics related to Access Link Control Application Part (ALCAP) protocol sessions associated with a Home-NodeB Gateway (HNB-GW) service instance configured and running on a system.

Product

HNBGW

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show alcap statistics [ alcap-service alcap_svc_name [ aal2-node aal2_node_name
 [ aal2-path aal2_path_id ] ] ] [ verbose ] [ | { grep grep_options | more } ]
```

name *alcap_svc_name*

Specifies the name of the ALCAP service for which statistics are to be displayed.

aal2-node *aal2-node*

Specifies the name of the ATM Adaptation Layer 2 (AAL2) node for which ALCAP service related statistics will be displayed.

aal2-path *aal2_path_id*

Specifies the identity number of the AAL2 path on a specific ATM Adaptation Layer 2 (AAL2) node for which ALCAP service statistics counters will be displayed.

| { 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 the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in *Command Line Interface Overview* chapter of the *Command Line Interface Reference*.

Usage Guidelines

This command is used to display the sessions statistics and counters for ALCAP service.

Example

The following command displays the service session statistics counters for ALCAP service named as *alcap_hnb_svc1*:

```
show alcap counters alcap-service alcap_hnb_svc1
```

Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

show apn

Displays configuration information for either a specific or all configured Access Point Names (APNs).

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show apn { all | name *apn_name* **} [| { grep** *grep_options* **| more }]**

all

Displays information on all APNs configured on the system.

name *apn_name*

Displays information for an APN specified as an alphanumeric string of 1 through 62 characters that is case sensitive.

| { 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** options, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage Guidelines

This command is used to verify the configuration of one or all APNs for monitoring or troubleshooting purposes. The output is a concise listing of APN parameter settings.

If this command is executed from within the local context with the all keyword, information for all APNs configured on the system will be displayed.

Example

The following command displays configuration information for all APNs:

```
show apn all
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show apn counters ip-allocation

Displays cumulative statistics of IP allocation method for calls set up so far, per Access Point Name (APN) basis.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show apn counters ip-allocation [all | name *apn_name* **] [| { grep** *grep_options* **| more }]**

all

Displays statistics for all APNs.

name *apn_name*

Displays statistics for the APN specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

| { 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.

Usage Guidelines

This command is used to display the cumulative IP allocation counters on a per APN basis. Output of this command gives the user clear idea of how many sessions in each APN have used a particular type of ip-allocation method.

If this command is issued from within the local context, the statistics displayed will be cumulative for all APNs configured on the system regardless of context. If no APN name is specified and the command is executed from a context with multiple APNs configured, the output will be cumulative for all APNs in the context.

Example

The following command displays statistics for all APN on a system:

```
show apn counter ip-allocation all
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show apn statistics

Displays statistics for either a specific Access Point Name (APN) or all configured APNs. Also can be used to display APN statistics at the ARP/QCI level.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show apn statistics [ all | name` *`apn_name`* **`]qci { all | 1-9 | non-std [ gbr | non-gbr ] } arp { all | 1-15 } ] [ | { grep`** *`grep_options`* **`| more } ]`**

all

Displays statistics for all APNs.

name *apn_name*

Displays statistics for the APN specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

qci

Enables the configuration of ARP priority level statistics for the specified QCI.

Important ARP Granularity and Per QCI Packet Drop Counters is a license-controlled feature. Contact your Cisco account or support representative for licensing details.

all

Configures the collection of ARP priority level statistics for all QCIs.

Important ARP Granularity and Per QCI Packet Drop Counters is a license-controlled feature. Contact your Cisco account or support representative for licensing details.

1-9

Configures the collection of ARP priority level statistics for a specific QCI 1 through 9.

Important ARP Granularity and Per QCI Packet Drop Counters is a license-controlled feature. Contact your Cisco account or support representative for licensing details.

non-std

Configures collection of ARP priority level statistics for non-standard non-guaranteed bit rate (GBR) QCIs.

Important ARP Granularity and Per QCI Packet Drop Counters is a license-controlled feature. Contact your Cisco account or support representative for licensing details.

non-gbr

Configures the collection of ARP priority level statistics for non-standard non-GBR QCIs.

Important ARP Granularity and Per QCI Packet Drop Counters is a license-controlled feature. Contact your Cisco account or support representative for licensing details.

gbr

Configures the collection of ARP priority level statistics for non-standard GBR QCIs.

Note ARP Granularity and Per QCI Packet Drop Counters is a license-controlled feature. Contact your Cisco account or support representative for licensing details.

arp

Configures the collection of ARP priority level statistics for the specified ARP.

Important ARP Granularity and Per QCI Packet Drop Counters is a license-controlled feature. Contact your Cisco account or support representative for licensing details.

1-15

Configures ARP priority level statistics for a specified ARP of 1 through 15.

Important ARP Granularity and Per QCI Packet Drop Counters is a license-controlled feature. Contact your Cisco account or support representative for licensing details.

| { 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.

Usage Guidelines

This command is used to view statistics for one or all APNs within a context for monitoring or troubleshooting purposes.

If this command is issued from within the local context, the statistics displayed will be cumulative for all APNs configured on the system regardless of context. If no APN name is specified and the command is executed from a context with multiple APNs configured, the output will be cumulative for all APNs in the context.

Example

The following command displays statistics for an APN named *isp2*:

```
show apn statistics name isp2
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show apn-profile

Displays information for configured Access Point Name (APN) profiles.

Product

MME

SGSN

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show apn-profile { all | full { all | name *apn_name* **} | name** *apn_name* **} [| { grep** *grep_options* **| more }]**

all

Lists all APN profiles configured on the system.

full { all | name *apn_name* }

full: Displays all information in the APN profile(s).

all: Displays full information for all APN profiles configured on the system.

name *apn_name*: Displays full information for an APN profile specified as an alphanumeric string of 1 through 64 characters.

name *apn_name*

Displays information for an APN profile specified as an alphanumeric string of 1 through 64 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.

Usage Guidelines Use this command to display information for APN profiles configured on the system. APN profiles are configured through the global configuration mode and in the APN profile configuration mode. For more information regarding APN profile commands, refer to the *APN Profile Configuration Mode Commands* chapter.

Example

The following command displays all available information for an APN profile named *apn-prof3*:

```
show apn-profile full name apn-prof3
```

show apn-remap-table

Displays information for Access Point Name (APN) remap tables configured on the system.

Product MME

SGSN

Privilege Inspector

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description **show apn-remap-table { all | full { all | name** *remap_table_name* **} | name** *remap_table_name* **} [| { grep** *grep_options* **| more }]**

all

Lists all APN remap tables configured on the system.

full { all | name *remap_table_name* }

full: Displays a full set (all) of available information for the configured APN remap table(s).

all: Displays the full set of available information for all APN remap tables configured on the system.

name *remap_table_name*: Displays the full set of available information for an existing APN remap table specified as alphanumeric string of 1 through 64 characters.

name *remap_table_name*

Displays information for an existing APN remap table specified as an alphanumeric string of 1 through 64 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.

Usage Guidelines

Use this command to display information for APN remap tables configured on the system. APN remap tables are configured through the Global Configuration mode and in the APN remap table configuration mode. For more information regarding APN remap table commands, refer to the *APN Remap Table Configuration Mode Commands* chapter.

Example

The following command displays all available information for an APN remap table named *remap-table12*:

```
show apn-remap-table full name remap-table12
```

show aps

Displays information for configured Automatic Protection Switching (APS) parameters.

Product

SGSN

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show aps { all | card-stats *slot_number* **[clear] | info** *slot_number/port_number* **| port-stats** *slot_number/port_number* **[clear] | port-status } [| { grep** *grep_options* **| more }]**

all

Lists APS information for all cards configured with APS.

card-stats*slot_number* [clear]

Displays the APS statistics for the identified card. If the **clear** keyword is included with the command, the APS statistics for the specified card are cleared (reset to zero).

slot_number is an integer that identifies the chassis slot holding the card.

info*slot_number/port_number*

Displays APS information for a specific port.

slot_number/port_number: The first number must be an integer that identifies the chassis slot holding the specified card. The slot number must be followed by a slash '/', which must be followed immediately by the port number - an integer from 1 to 4 depending upon the type of card.

port-stats*slot_number/port_number* [clear]

Displays APS statistics for a specific port. If the **clear** keyword is included with the command then the APS statistics for the specified port are cleared (reset to zero).

slot_number/port_number: The first number must be an integer from 1 to 48 to identify the chassis slot holding the specified card. The slot number must be followed by a slash '/', which must be followed immediately by the port number - an integer from 1 to 4 depending upon the type of card.

port-status*slot_number/port_number*

Displays APS status information for a specific port.

slot_number/port_number: The first number must be an integer from 1 to 48 to identify the chassis slot holding the specified card. The slot number must be followed by a slash '/', which must be followed immediately by the port number - an integer from 1 to 4 depending upon the type of card.

| { 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.

Usage Guidelines

Use this command to display APS redundancy configuration, APS card and port status, and APS card and port statistics. APS is configured at the card level. For details on configuring APS, refer to the *Card Configuration Mode Commands* chapter in this reference.

Important

APS is only relevant for the CLC2 and OLC2 line cards supporting SONET/SDH.

Example

The following command displays all available APS configuration information for a specific port 1 on the line card in slot 27:

```
show aps info 27/1
```

show asngw-service

Displays information about selected Access Service Network Gateway (ASN-GW) calls/services.

Product

ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show asngw-service { all | name *service_name* **| session | statistics } [bs-status [address** *ip_address* **| filter { all | icmp-monitored | no-calls | summary | up]] [| { grep** *grep_options* **| more }]**

all

Displays information for all configured ASN-GW services.

name *service_name*

Displays information only for an existing ASN-GW service in the current context specified as an alphanumeric string of 1 through 63 characters.

session

Displays information about configured ASN-GW sessions. See the **show asngw-service session** command

statistics

Total of collected information for specific protocol since the last **restart** or **clear** command.

bs-status { address *ip_address* | filter { all | icmp-monitored | no-calls | summary | up } }

Displays the ASN base station (BS) status based on IP address and various filters.

address *ip_address* specifies the IP address of ASN base station whose status is requested. *ip_address* must be entered in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

filter { all | icmp-monitored | no-calls | summary | up }: Filters the requested BS's status on the basis of following criteria:

- **all**: Displays the status of all ASN base stations.
- **icmp-monitored**: Displays the status of ASN base stations that are monitored through ICMP ping messages.
- **no-calls**: Displays the status of an ASN base station that has no active calls.
- **summary**: Displays a summary of the status of requested ASN base stations.
- **up**: Displays the of status of ASN base stations that are in active state.

| { 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.

Usage Guidelines

Use this command to view information for selected configured ASN-GW services.

Example

The following command displays available information for all active ASN-GW services.

```
show asngw-service all
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show asngw-service session

Displays statistics for specific Access Service Network Gateway (ASN-GW) sessions.

Product

ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show asngw-service session [all | anchor-only [full] | callid *call_id* **| counters | full | ip-address** *ipv4_address* **| msid** *msid_number* **| non-anchor-only [full] | peer-address** *ipv4_address* **| summary | username** *user_name* **] [| { grep** *grep_options* **| more }]**

all

Displays all related information for all active ASN-GW service sessions.

anchor-only

Displays all available information for all active ASN-GW service sessions on an anchor ASN-GW only.

callid *call_id*

Displays available information for the call identification number specified as an 8-digit hexadecimal number.

full

Displays all available information for the associated display or filter keyword.

ip-address *ipv4_address*

Specifies the IP address of the subscriber in IPv4 dotted-decimal notation.

msid *msid_number*

Displays available information for the specific mobile station identification number (MSID).

non-anchor-only

Displays all available information for all active ASN-GW service sessions on a non-anchor ASN-GW only.

peer-address *ipv4_address*

Specifies the Ip address of an IP peer in dotted-decimal notation.

summary

Displays summary of available information for associated display or filter keyword (previous keyword).

username *user_name*

Specifies the name of a user within current context as an alphanumeric string of 1 through 127 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.

Usage Guidelines

Use this command to view configuration information for an ASN-GW session.

Example

The following command displays all available ASN-GW sessions.

```
show asngw-service session all
```

Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

show asngw-service session counters

Displays statistics for specific Access Service Network Gateway (ASN-GW) sessions.

Product

ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show asngw-service session counters [ [ function-type { auth-relay |
context-transfer | data-path | handoff | im-operation | ms-state-change |
paging | qos } ] | [ anchor-only | callid call_id | ip-address ipv4_address |
msid msid_number | non-anchor-only | peer-address ipv4_address | username user_name
 ] [ r4-only | r6-only | verbose ] ] [ | { grep grep_options | more } ]
```

anchor-only

Displays all available information for all active anchor sessions in an ASN-GW service.

callid *call_id*

Displays available information for the call identification number specified as an 8-digit hexadecimal number.

function-type { auth-relay | context-transfer | data-path | handoff | im-operation | ms-state-change | paging | qos }

Displays the counters for specific type of functions in an ASN-GW session.

auth-relay: Displays information about authentication relay messages.

context-transfer: Displays information about context-transfer messages.

data-path: Displays information about data-path registration messages.

handoff: Displays information about hand-off messages.

im-operations: Displays information about idle mode state operation messages.

ms-state-change: Displays information about MS state change messages.

paging: Displays information about paging messages.

qos: Displays information about RR messages.

ip-address *ipv4_address*

Specifies the IP address of the subscriber in IPv4 dotted-decimal notation.

msid *msid_number*

Displays available information for the specific mobile station identification (MSID) number.

non-anchor-only

Displays all available information for all active non-anchor sessions in an ASN-GW service.

peer-address *ipv4_address*

Specifies the IP address of an IP peer in IPv4 dotted-decimal notation.

r6-only

Displays all available counters for R6 interface in an ASN-GW session.

r4-only

Displays all available counters for R4 interface in an ASN-GW session.

username *user_name*

Displays available session information for the specific WiMAX user in ASN-GW service session.

user_name is an alphanumeric string of 1 through 127 characters.

verbose

Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

| { 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.

Usage Guidelines

Use this command to view the counters of an ASN-GW session.

Example

The following command displays the counters for data path type function.

```
show asngw-service session counters function-type data-path
```

Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

show asngw-service statistics

Displays statistics for all Access Service Network Gateway (ASN-GW) sessions.

Product

ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show asngw-service statistics [function-type { auth-relay | context-transfer | data-path | handoff | im-operations | ms-state-change | paging | qos | capability }] [name *service_name* **| r4-only | r6-only | verbose | peer-address** *ipv4_address* **] [peer-id** *id* **][verbose] [{ grep** *grep_options* **| more** }]

function-type

Displays information about selected function type on R4 or R6 interface.

function-type { auth-relay | context-transfer | data-path | handoff | im-operations | ms-state-change | paging | qos | capability} [r4-only | r6-only]

Displays the counters for specific type of functions in an ASN-GW session.

auth-relay: Displays information about authentication relay messages.

context-transfer: Displays information about context-transfer messages.

data-path: Displays information about data-path registration messages.

handoff: Displays information about hand-off messages.

im-operations: Displays information about idle mode state operation messages.

ms-state-change: Displays information about MS state change messages.

paging: Displays information about paging messages.

qos: Displays information about RR messages.

capability: Displays the capability negotiation between the ASNGW and the base station.

r4-only: Displays information about selected function on R4 interface.

r6-only: Displays information about selected function on R6 interface.

name *service_name*

Displays information for an existing service specified as an alphanumeric string of 1 through 63 characters.

r4-only

Displays statistics of R4 interface in ASN-GW services.

r6-only

Displays statistics of R6 interface in ASN-GW services.

peer-address *ipv4_address*

Specifies the IP address of an IP Peer in IPv4 dotted-decimal notation.

peer-id < *id* >

Display the statistics based on the 6-byte BSID or ASNGW ID in addition to the IPv4 address.

verbose

Specifies that the output should display all available information. If this option is not specified then the output will be the standard level which is the concise mode.

| { 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.

Usage Guidelines Use this command to display ASN-GW statistics.

Example

The following command displays information about selected MS-State-Change function.

```
show asngw-service statistics function-type ms-state-change
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show asnpc-service

Displays information about selected Access Service Network Paging Controller and Location Registry (ASN PC/LR) services.

Product ASN-GW

Privilege Security Administrator, Administrator, Operator, Inspector

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show asnpc-service { all | id | name service_name | session | statistics }
[ | { grep grep_options | more } ]
```

all

Displays information for all configured ASN PC services.

paging-group

Displays all the configured paging-groups and associated paging nodes, and the offset count. For a specific paging group, enter the paging group id number.

name *service_name*

Displays information only for an existing ASN PC service specified as an alphanumeric string of 1 through 63 characters.

session

Displays information about configured ASN PC sessions.

statistics

Total of collected information for specific protocol since last restart or clear command.

| { 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.

Usage Guidelines

Use this command to view information for selected configured ASN PC services.

Example

The following command displays available information for all active ASN PC services.

```
show asnpc-service all
```

Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

show asnpc-service session

Displays statistics for specific Access Service Network Paging Controller (ASN PC) service sessions.

Product

ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show asnpc-service session [all | callid *call_id* **| counters | full | msid** *msid_number* **| peer-address** *ipv4_address* **| summary] [| { grep** *grep_options* **| more }]**

all

Displays all related information for all active ASN PC service sessions.

callid *call_id*

Displays available information for the call identification number specified as an 8-digit hexadecimal number.

full

Displays all available information for the associated display or filter keyword.

msid *msid_number*

Displays available information for the specific mobile station identification (MSID) number.

peer-address *ipv4_address*

Specifies the IP address of an IP peer in IPv4 dotted-decimal notation.

summary

Displays summary of available information for associated display or filter keyword (previous keyword).

| { 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.

Usage Guidelines

Use this command to view configuration information for an ASN PC session.

Example

The following command displays all available ASN PC session counters in verbose mode.

```
show asnpc-service session all
```

The following command displays full ASN PC session counters in verbose mode.

```
show asnpc-service session full
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show asnpc-service session counters

Displays session counters for Access Service Network Paging Controller (ASN PC) service sessions.

Product

ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show asngw-service session counters [all | callid *call_id* **| msid** *msid_number* **| peer-address** *ipv4_address* **| verbose]] [| { grep** *grep_options* **| more }]**

all

Displays all available counters for all ASN PC service sessions.

callid *call_id*

Displays available information for the call identification number specified as an 8-digit hexadecimal number.

msid *msid_number*

Displays available information for the specific mobile station identification (MSID) number.

peer-address *ipv4_address*

Specifies the IP address of an IP peer in IPv4 dotted-decimal notation.

verbose

Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

| { 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.

Usage Guidelines

Use this command to view the counters of an ASN PC session.

Example

The following command displays the counters for ASN PC service sessions in verbose mode.

```
show asnpc-service session counters verbose
```

Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

show asnpc-service session counters verbose

Displays session counters for Access Service Network Paging Controller (ASN PC) service sessions in complete detail.

Product

ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show asngw-service session counters verbose [function-type { context-transfer | im-operations | ms-state-change | paging }] [all | callid *call_id* **| msid** *msid_number* **| peer-address** *ipv4_address* **]] [| { grep** *grep_options* **| more }]**

all

Displays all available counters for all ASN PC service sessions in verbose mode.

callid *call_id*

Displays full information for the call identification number specified as an 8-digit hexadecimal number.

function-type { context-transfer | im-operations | ms-state-change | paging }

Displays the counters for specific type of functions in an ASN-GW session.

context-transfer: Displays information about context-transfer messages.

im-operations: Displays information about idle mode state operation messages.

ms-state-change: Displays information about MS state change messages.

paging: Displays information about paging messages.

msid *msid_number*

Displays full information for the specific mobile station identification (MSID) number.

peer-address *ipv4_address*

Specifies the IP address of an IP peer IPv4 dotted-decimal notation.

r4-only

Displays statistics of R4 interface in ASN PC services in verbose mode.

r6-only

Displays statistics of R6 interface in ASN PC services in verbose mode.

| { 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.

Usage Guidelines

Use this command to view the counters of an ASN PC session in verbose mode.

Example

The following command displays the counters for data path type function.

```
show asnpc-service session counters verbose
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show asnpc-service statistics

Displays statistics for all ASN PC service sessions.

Product ASN-GW

Privilege Security Administrator, Administrator, Operator, Inspector

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show asnpc-service statistics [ name service_name | peer-address ipv4_address
 | verbose ]  [ r4-only | r6-only [ | { grep grep_options | more } ]
```

name *service_name*

Specifies an existing service name as an alphanumeric string of 1 through 63 characters.

peer-address *ipv4_address*

Specifies the IP address of an IP peer in IPv4 dotted-decimal notation.

verbose

Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

| { 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.

Usage Guidelines Use this command to display ASN PC statistics.

Example

The following command displays information about ASN PC service in verbose mode.

```
show asnpc-service statistics verbose
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show asnpc-service statistics verbose

Displays statistics for all Access Service Network Paging Controller (ASN PC) service in verbose mode.

Product ASN-GW

Privilege Security Administrator, Administrator, Operator, Inspector

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show asnpc-service statistics verbose [ function-type { context-transfer
 | im-operations | ms-state-change | paging } ] | all | r4-only | r6-only
 ] [ | { grep grep_options | more } ]
```

function-type { context-transfer | ms-state-change | paging }

Displays the statistics for specific type of functions in an ASN PC service in verbose mode.

context-transfer: Displays information about context-transfer messages.

im-operations: Displays information about idle mode state operation messages.

ms-state-change: Displays information about MS state change messages.

paging: Displays information about paging messages.

all

Displays statistics of all ASN PC services in verbose mode.

r4-only

Displays statistics of R4 interface in ASN PC services.

r6-only

Displays statistics of R6 interface in ASN PC services.

| { 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.

Usage Guidelines

Use this command to display ASN PC service statistics in verbose mode.

Example

The following command displays information about selected MS-State-Change function.

```
show asnpc-service statistics verbose function-type ms-state-change
```

Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

show banner

Displays the configured banner message for the current context.

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

```
show banner { all | charging-service | motd | lawful-intercept | pre-login
 } [ | { grep grep_options | more } ]
```

all

Displays all banners configured for a service in a system including the enhanced charging service (ECS).

charging-service

Displays banner message configured for an enhanced charging service in the current context.

motd

Display the banner message that is configured for the current context.

lawful-intercept

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.

| { 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.

Usage Guidelines

Show the configured banner to verify the message of the day contents for possible change

Example

The following command displays all current banner messages:

```
show banner all
```

show bcmcs counters

Displays Broadcast and Multicast Service (BCMCS)-specific counters and statistics.

Product

PDSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show bcmcs counters { all | callid *call_id* **| flow-id** *flow_id* **}**

all

Displays BCMCS-specific counters and statistics for all multicast sessions.

callid *call_id*

Displays BCMCS-specific counters and statistics for a specific call ID.

flow_id *flow_id*

Displays BCMCS-specific counters and statistics for a specific BCMCS flow, defined by a flow ID.

Usage Guidelines

Use this command to view BCMCS-specific statistics. You may narrow the results of the command output by specifying a specific call ID or flow ID.

Example

The following command displays all BCMCS counters:

```
show bcmcs counters all
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show bcmcs statistics

Displays Broadcast and Multicast Service (BCMCS)-specific statistics for the current PDSN-service.

Product PDSN

Privilege Security Administrator, Administrator, Operator, Inspector

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description **show bcmcs statistics [pdsn-service** *service_name* **]**

pdsn-service *service_name*

Defines a specific PDSN service from which to gather BCMCS-specific statistics.

Usage Guidelines Shows several sets of BCMCS-specific statistics, and may be configured to show statistics only for a certain PDSN service.

Example

The following command displays BCMCS statistics for the PDSN service named *group_1*:

```
show bcmcs statistics pdsn-service group_1
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show bfd

Displays Bidirectional Forwarding Detection (BFD) neighbors and their current debug settings.

Product PDSN

Privilege Security Administrator, Administrator, Operator, Inspector

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show bfd { debugging | neighbors }

show bfd debugging

Displays current BFD options for peer control messaging.

show bfd neighbors

Displays summary information for BFD-enabled neighbors.

Usage Guidelines

Show the configuration of BFD-enabled neighbors and the current debug settings.

Example

The following command displays information for BFD-enabled neighbors:

show bfd neighbors

Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

show boot

Displays information on the current boot image in use.

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

show boot [initial-config | { grep *grep_options* **| more }]**

initial-config

Identifies the OS image, configuration file, and boot priority used during the initial start up of the system.

| { 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.

Usage Guidelines

Show the boot information in preparing for maintenance activities by verifying current boot data. The boot image in use may not be the same as the boot image stored on the SPC/SMC due to upgrades and pending

reboots. **show boot initial-config** displays the actual boot image and configuration file loaded during boot. This may or may not be the highest priority image and makes this command useful when comparing the loaded image to the priority list.

Important This command is not supported on all platforms.

Example

The following command displays the boot system configuration priority list:

```
show boot
```

The following command displays the initial configuration after a system boot:

```
show boot initial-config
```

show bssap+ statistics

Displays Base Station system Application Part (BSSAP+) protocol statistics for the Gs interface between the SGSN and the Mobile services Switching Centre, Visitor Location Register (MSC/VLR).

Product SGSN

Privilege Inspector

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show bssap+ statistics [ gs-service gs_svc_name ] [ vlr { isdn-number ISDN_Num|
 name  vlr_name } ] [ verbose ] [ | { grep grep_options | more } ]
```

gs-service *gs_svc_name*

Specifies the name of a specific Gs service to filter the BSSAP+ information as an alphanumeric string of 1 through 63 characters that is case sensitive.

vlr { isdn-number *ISDN_Num*| name *vlr_name*

Identifies a specific VLR (by name or ISDN number) to filter BSSAP+ information.

vlr_name is the configured name of the VLR expressed.

VLR_num is the configured E.164-type ISDN number for the VLR. Enter a numerical string of 1 to 15 digits.

verbose

Indicates the output should provide as much information as possible. If this option is not specified then the output will be limited to a concise summary.

| { 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.

Usage Guidelines

Use this command to display the BSSAP+ statistics for the SGSN's Gs interface(s). Based on how the command is entered, this command displays collected BSSAP+ protocol statistics for the entire SGSN or for a specified Gs interface. Using the keywords of this command, the interface can be identified by defining a specific VLR connected to the SGSN or by identifying the Gs service to which the interface has been configured.

Example

The following command displays all BSSAP+ information for the Gs interface configured for the Gs service named *gssvc1*.

```
show bssap+ statistics gs-service gssvc1 verbose
```

Important Descriptions for show command outputs are available in the ***Statistics and Counters Reference***.

show bssgp statistics

Displays base station subsystem GPRS protocol statistics for traffic between the base station subsystem (BSS) and the SGSN over the Gb interface.

Product

SGSN

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show bssgp statistics [ gprs-service gprs_svc_name  | nse nse_id [ bvc bvc_id
 [ sessmgr | verbose ] ] ] [ verbose ] [ | { grep grep_options | more } ]
```

gprs-service *gprs_svc_name*

Specifies the name of an existing GPRS service for which the BSSGP information will be filtered as an alphanumeric string of 1 through 63 characters that is case-sensitive.

nse*nse_ID*

Enter this keyword to display the BSSGP statistics for the network service entity (NSE) specified as an integer from 0 through 65535.

bvc*bvc_ID*

Enter this keyword to display the BSSGP statistics for the BSSGP virtual connection (BVC) specified as an integer from 0 through 6500.

sessmgr instance *sessmgr_instance_number*

Enter this keyword to display the BSSGP statistics for a session manager instance specified as an integer from 1 through 4294967295.

verbose

Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

| { 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.

Usage Guidelines

Use this command to display the BBSGP statistics for a particular GPRS service or NSEI.

Example

The following command displays BSSGP statistics for the GPRS service named *gprs1*.

```
show bssgp statistics gprs-service gprs1
```

Important

Descriptions for show command outputs are available in the ***Statistics and Counters Reference***.

show bssgp status

Displays the traffic status through the BSSGP (base station subsystem GPRS protocol) layer between the base station subsystem (BSS) and the SGSN over the Gb interface.

Product

SGSN

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show bssgp status { bvc-bucket nsei nse_id bvci bvc_id | bvc-stat nsei nse_id
 bvci bvc_id } [ | { grep grep_options | more } ]
```

bvc-bucket nsei*nse_id* bvci *bvc_id*

Displays traffic status for a specific BVC bucket identified by the NSEI (network service entity ID) and BVCI (BSSGP virtual connection ID).

nse_ID is an integer from 0 through 65535.

bvc_ID is an integer from 0 through 65000.

bvc-stat nsei*nse_id* bvci *bvc_id*

Displays traffic status for a BVC identified by the NSEI (network service entity ID) and BVCI (BSSGP virtual connection ID).

nse_ID is an integer from 0 through 65535.

bvc_ID is an integer from 0 through 65000.

| { 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.

Usage Guidelines

Use this command to display BVC status of the BBSGP layer for specified NSEI and BVCI.

Example

The following command displays BSSGP traffic status for the BVC bucket for NSEI *2556* BVCI *241*.

```
show bssgp status bvc-bucket nsei 2556 bvci 241
```

Important

Descriptions for show command outputs are available in the ***Statistics and Counters Reference***.

show build

Displays detailed information about the currently active StarOS release build.

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

```
show build [ | { grep grep_options | more } ] ]
```

| { 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 information on usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage Guidelines

Use this command to display detailed information on the currently active StarOS release build.

Example

The following command displays StarOS build information:

```
show build
```

show bulkstats

Displays information on bulk statistics.

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

```
show bulkstats [ [ data ] | [ schemas ] | [ variables [ schema_name ] [
obsolete ] ] [ | { grep grep_options | more } ] ]
```

data

Displays collected bulk statistical data.

schema

Displays the configuration of the statistics to be collected on a per-schema basis.

Important

For information on available schemas, refer to the *Bulk Statistics Configuration Mode Commands* chapter.

variables *schema_name*

Displays all valid bulkstat schema statistics, or only the statistics for the specified schema.

schema_name specifies the name of the schemas available on system. The following is the list of available schemas in this release.

- aal2

- alcap
- apn
- asngw
- asnpc
- bcmcs
- card
- closedrp
- common
- context
- cs-network-ranap
- cs-network-rtp
- cs-network-sccp
- cscf
- cscfintf
- dcca
- dcca-group
- diameter-acct
- diameter-auth
- diameter-acct
- dlci-util
- dpca
- ecs
- egtpc
- epdg
- fa
- flow-kpi
- fng
- gprs
- gtpc
- gtpp
- gtpu
- ha
- henbgw-access

Important In Release 20, 21.0 and 21.1, HeNBGW is not supported. For more information, contact your Cisco account representative.

- henbgw-network

Important In Release 20, 21.0 and 21.1, HeNBGW is not supported. For more information, contact your Cisco account representative.

- hnbgw-hnbap

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- hnbgw-hnbap-access-closed

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- hnbgw-hnbap-access-hybrid

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- hnbgw-hnbap-access-open

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- hnbgw-iubc-sabp

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- hnbgw-iubc-tcp

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- hnbgw-ranap

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- hnbgw-ranap-access-closed

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- hnbgw-ranap-access-hybrid

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- hnbgw-ranap-access-open

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- hnbgw-rtp

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- hnbgw-rtp-access-closed

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- hnbgw-rtp-access-hybrid

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- hnbgw-rtp-access-open

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- hnbgw-rua

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- hnbgw-rua-access-closed

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- hnbgw-rua-access-hybrid

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- hnbgw-rua-access-open

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- hnbgw-sabp

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- hnbgw-sabp-access-closed

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- hnbgw-sabp-access-hybrid

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- hnbgw-sabp-access-open

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- hnbgw-sctp

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- hsgw
- hss
- icsr
- imsa
- ippool
- ipsg
- lac
- lcs
- link-aggr
- lma
- lns
- mag
- map
- mipv6ha
- mme
- mvs
- nat-realm
- p2p
- pcc-af
- pcc-policy
- pcc-quota
- pcc-service
- pcc-sp-endpt
- pdg
- pdif
- pgw
- phsgw
- phspc
- port
- ppp
- ps-network-gtpu
- ps-network-ranap
- ps-network-sccp
- radius
- radius-group

- readdress-server
- rlf
- rlf-detailed
- rp
- rulebase
- samog
- sbc
- sccp
- sgs
- sgs-vlr
- sgsn
- sgtp
- sgw
- sls
- ss7link
- ss7rd
- system
- tai
- vlan-npu
- vpn
- wsg

obsolete

This keyword shows obsolete (but still available) schema variables. An asterisk (*) is displayed next to schema variables that have been obsoleted.

| { 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 information on usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage Guidelines

Use this command to display information on bulk statistics supported by the system.

The **variable** keyword can be used to list statistics supported by the system either for all schemas, or for an individual schema.

The **schema** keyword can be used to display the configuration of settings for bulk statistics, including the schema.

The **data** keyword can be used to display bulk statistic data collected up to that point.

Example

The following command displays bulk statistics data:

```
show bulkstats data
```

The following command displays bulk statistics schema configuration:

```
show bulkstats data schemas
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show ca-certificate

Displays information for Certificate Authority (CA) digital certificates configured on this system.

Product All

Privilege Inspector

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show ca-certificate { all | name name }
```

all

Displays information about all the configured CA certificates.

name *name*

Displays information about an existing configured CA certificate name specified as n alphanumeric string of 1 through 128 characters.

Usage Guidelines View information for CA certificates configured on this system.

Example

The following command displays information for a CA certificate named *cert-1*:

```
show ca-certificate name cert-1
```

Important Output descriptions for some commands are available in the *Statistics and Counters Reference*.

show ca-crl

Displays information for Certificate Authority (CA) Certificate Revocation List (CRL) configured on this system.

Product All

Privilege Inspector

Command Modes Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description **`show ca-crl { all | name`** *`name`* **`}`**

all

Displays information about all the configured CA-CRLs.

name *name*

Displays information about an existing CA-CRL name specified as an alphanumeric string of 1 through 128 characters.

Usage Guidelines View information for CA-CRLs on this system.

Example

The following command displays information for a CA-CRL named *crl-5*:

```
show ca-crl name crl-5
```

Important Output descriptions for some commands are available in the *Statistics and Counters Reference*.

show cae-group server

Displays configuration information, including the name of the associated CAE group, for all CAEs or for a specific CAE. The CAE (Content Adaptation Engine) is an optional component of the Mobile Videoscape.

Important In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

Product MVG

Privilege Security Administrator, Administrator

Command Modes Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description **show cae-group server { all | name** *cae_name* **}**

all

Shows the configuration information, including the associated CAE group, for all CAEs.

name *cae_name*

Shows the configuration information for a specific CAE.

Usage Guidelines Use this command to display configuration information for all CAEs or for a specific CAE. This command can be issued from either the local context or the context in which the associated CAE group is defined.

Example

The following command displays configuration information for the CAE named *server_1*:

```
show cae-group server name server_1
```

show call-control-profile

Displays information for call control profiles configured on the system.

Product MME

SGSN

Privilege Inspector

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description **show call-control-profile { all | full { all | name** *profile_name* **} | name** *profile_name* **} [| { grep** *grep_options* **| more }]**

all

Lists all call-control profiles configured on the system.

full { all | name *profile_name* }

full: Displays a full set (all) of available information in the call-control profile.

all: Displays a full set of available information for all call-control profiles configured on the system.

name *profile_name*: Displays full information for an existing call-control profile specified as an alphanumeric string of 1 through 64 characters.

name *profile_name*

Displays information for an existing call-control profile specified as an alphanumeric string of 1 through 64 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.

Usage Guidelines

Use this command to display information for call-control profiles configured on the system. Call-control profiles are configured through the global configuration mode and in the call-control profile configuration mode. For more information regarding call-control profile commands, refer to the *Call-Control Profile Configuration Mode Commands* chapter.

Example

The following command displays all available information for a call-control profile named *call-prof2*:

```
show call-control-profile full name call-prof2
```

show call-home

Displays information for Smart Call Home settings configured on the system.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show call-home [alert-group | detail | mail-server status | profile [all | name *profile_name* **] | statistics [| { grep** *grep_options* **| more }]]**

alert-group

Displays information for all alert groups configured on the system. It also indicates if an alert-group has been disabled by the user.

detail

Displays general information and alert-group settings for all configured call-home profiles.

mail-server status

Displays status information for call-home mail servers that are configured on the system.

profile { all | name *profile_name* }

Displays all available information for all call-home profiles on the system or a specified call-home profile.

all: Displays all available information for all call-home profiles configured on the system.

name *profile_name*: Displays all available information for an existing call-home profile specified as an alphanumeric string of 1 through 31 characters.

name *profile_name*

Displays information for a call-home profile specified as an alphanumeric string of 1 through 31 characters.

statistics

Displays statistical information for call-home statistics configured on the system.

| { 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.

Usage Guidelines

Use this command to display profile and notification policy information associated with the call-home profiles configured on the system. Call-home profiles are configured through the Context Configuration Mode and in the Call-home Configuration Mode. For more information regarding call-home commands, refer to the *Call Control Profile Configuration Mode Commands* chapter.

Example

The following command displays all available information for a call-home profile named *call-home-prof1*:

```
show call-home profile name call-home-prof1
```

show camel-service

Displays configuration details for Customized Applications for Mobile networks Enhanced Logic (CAMEL) services configured for this SGSN.

Product

SGSN

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show camel-service { all | name service_name } [ | grep grep_options | more ]
```

all

Displays the configuration details for all configured CAMEL services.

name

Displays the configuration details for an existing CAMEL service specified 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.

Usage Guidelines

View configuration information for CAMEL services.

Example

The following command displays the configuration information for a CAMEL service identified as *camel4sgsnTO*:

```
show camel-service name camel4sgsnTO
```

Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

show card

Displays various types of information for a card or all cards in the system.

Product

All

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show card { diag [*slot#* **] | hardware [** *slot#* **] | info [** *slot#* **] | mappings | table [all] } [| { grep** *grep_options* **| more }]**

diag

Displays diagnostic results for a specific card or all cards.

hardware

Displays information about installed hardware.

info

Displays detailed information for a specific card or all cards

mappings

Displays mappings between front-installed application cards and rear-installed interface cards.

Important This keyword is only supported on the ASR 5000.

table [all]

Displays information about each card in tabular output. The **all** option includes empty slots in the output.

slot#

Specifies the slot number for a card as an integer from 1 through 48.

| { 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.

Usage Guidelines Use this command to view various types of information for all cards or a a specified card.

Example

The following command displays diagnostic information for the card in slot 1:

```
show card diag 1
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show cbs counters

Important In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Displays counters associated with cell broadcasting service (CBS).

Product

HNBGW

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show cbs counters [cbs-service *cbs_service_name* **] [| { grep** *grep_options* **| more }]**

cbs-service *cbs_service_name*

Displays information for specific CBS service. *cbs_service_name* is a string of size 1 through 63.

| { 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.

Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

Usage Guidelines

Use this command to display the counters for CBS service

Example

The following command displays the counters for the CBS named *my_service*:

```
show cbs counters cbc-service my_service
```

show cbs sessions

Important

In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

This command displays the information for CBS sessions.

Product

HNBGW

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show cbs sessions [all] [cbc-address *cbc_address* **| cbs-service** *cbs_service_name* **] [[full | summary] [cbc-address** *cbc_address* **| cbs-service** *cbs_service_name* **]] [| { grep** *grep_options* **| more }]**

all

Displays all CBS sessions.

cbc-address *cbc_address*

Specifies the IP address of a Cell Broadcast Center (CBC) in IPv4 dotted-decimal notation.

cbs-service *cbs_service_name*

Displays information for a named CBS service. *cbs_service_name* is an alphanumeric string of 1 through 63 characters.

full

Displays all available session information.

summary

Displays summary information for CBS sessions

| { 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.

Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

Usage Guidelines

Use this command to display the information for CBS sessions.

Example

The following command displays the full session information for CBS address *101.102.109.211*:

```
show cbs sessions full cbc-address 101.102.109.211
```

show cbs statistics

Important In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Displays CBS statistics.

Product

HNBGW

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

show cbs statistics [cbc-address *cbc_address* **| cbs-service** *cbs_service_name* **] [sabp-only | tcp-only | verbose] [| { grep** *grep_options* **| more }]**

cbc-address *cbc_address*

Designates the IP address of a CBC in IPv4 dotted-decimal notation.

cbs-service *cbs_service_name*

Displays information for a named CBS service. *cbs_service_name* is an alphanumeric string of 1 through 63 characters.

sabp-only

Displays Service Area Broadcast Protocol (SABP) statistics for the selected CBS Service.

tcp-only

Displays TCP statistics for the selected CBS Service.

verbose

Displays more detailed CBS statistics.

| { 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.

Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

Usage Guidelines

Use this command to display the statistics for CB service.

Example

The following command displays the SABP statistics for the CBC at *101.102.109.211*:

```
show cbs statistics cbc-address 101.102.109.211 sabp-only
```

show cbs-service

Important In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Displays information for all or a specific CBS service.

Product

HNBGW

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show cbs-service { all | name` *`cbs_service_name`* **`} [ status ] [ | { grep`** *`grep_options`* **`| more } ]`**

all

Displays all CBS services.

name*cbs_service_name*

Displays information for named CBS service.*cbs_service_name* is an alphanumeric string of 1 through 63 characters.

status

Display detailed status.

| { 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.

Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

Usage Guidelines

Use this command to display the information for all or a specific CBS service.

Example

The following command displays the detailed status of a CBS service with name*my_service*:

```
show cbs-service name my_service status
```

show cdr

Displays information about Charging Data Records (CDRs).

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show cdr { file-space-usage | statistics } [ | { grep` *`grep_options`* **`| more } ]`**

file-space-usage

Displays the amount of file space used by Charging Data Record (CDR) files.

statistics

Displays CDR file statistics.

| { 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.

Usage Guidelines

Use this command to view CDR flow control information.

Example

The following command displays CDR files statistics:

```
show cdr statistics
```

The following command displays the amount of file space used by the CDR files:

```
show cdr file-space-usage
```

Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

show certificate

Displays information about the certificates configured on this system.

Product

All

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show certificate { all | name` *`name`* **`}`**

all

Displays information about all the configured certificates on this system.

name *name*

Displays information of a specified certificate configured.

name must be the name of an existing certificate specified as an alphanumeric string of 1 through 128 characters.

Usage Guidelines

View information for local node certificates on this system.

Example

The following command displays information for a node certificate named *certificate-3*:

```
show certificate name certificate-3
```

Important

Output descriptions for some commands are available in the *Statistics and Counters Reference*.

show cgw-service

Displays configuration and/or statistical information for CGW services on this system.

Product

SaMOG

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax Description

`show cgw-service { all | name` *`name`* **`| statistics { all [ verbose ] [ | { grep`** *`grep_options`* **`| more } ] | name`** *`name`*`}` **`[ | { grep`** *`grep_options`* **`| more } ]`**

all

Displays all CGW services.

name *name*

Displays information for an existing CGW service specified as an alphanumeric string of 1 through 63 characters.

statistics

Displays node level Statistics for CGW.

verbose

Specifies detailed statistics.

| { 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.

Usage Guidelines

Use this command to displays configuration and/or statistical information for CGW services on this system.

Example

The following command displays information for all CGW services:

```
show cgw-service all
```

show cli

Displays current or historical information about command line interface (CLI) user session(s).

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

```
show cli { configuration-monitor | history [ all | exclude-show ] | session }
[ | { grep grep_options | more } ]
```

configuration-monitor

Displays information related to the **cli configuration-monitor** command, including the number of seconds remaining until the next configuration monitor check is performed.

history [all | exclude-show]

Displays CLI command history for this CLI session when another option is not selected.

all: Displays the CLI command history for all CLI sessions.

exclude-show: Excludes **show** commands.

session

Displays information about the current CLI session.

| { 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.

Usage Guidelines

Displays current or historical CLI sessions, This command is useful when there is some unexpected output from a chassis and a check of current CLI users may reveal other in-progress activities that may have contributed to the anomaly.

Example

The following command displays information about all current CLI sessions:

```
show cli
```

show clock

Displays the current system data and time.

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

show clock [universal] [| { grep *grep_options* **| more }]**

universal

Displays the date and time in universal coordinated time (UTC/GMT) format.

| { 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 Output* section of the *Command Line Interface Overview* chapter.

Usage Guidelines

Check the current time of a chassis to compare with network wide time or for logging purposes if network accounting and/or event records appear to have inconsistent timestamps.

Important This command is not supported on all platforms.

Example

The following displays the system time in local time and UTC, respectively.

```
show clock
show clock universal
```

show cloud configuration

Displays the contents of the configuration file.

Product VPC

Privilege Security Administrator, Administrator, Inspector, Operator

Mode

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax

```
show cloud configuration
```

Usage

This command dumps the contents of the configuration file to the screen. It displays the configuration file on the config disk or the local flash. Usually the user does not have direct access to these files. The local param file on the flash is defined during the VPC installation and the config disk is usually created by the orchestrator and then attached to the card.

Example

This command displays the hardware configuration associated with card number 1:

```
show cloud configuration
```

show cloud hardware

Displays information regarding the configuration for each card or a specific card.

Product

VPC

Privilege

Security Administrator, Administrator, Inspector, Operator

Mode

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax

show cloud hardware [**iftask** | **optimum** | **test**] [*card_number*]

iftask

Displays IFTASK information.

optimum

Displays the optimum configuration of the underlying VM hardware according to the available parameters. It provides information regarding the configured vCPU, memory size, huge page size, crypto hardware and the NIC.

test

Compares the configuration of the underlying VM hardware of a specific card or all cards in the VPC to the optimum configuration. It provides information regarding the configured vCPU, memory size, huge page size, crypto hardware and the NIC and indicates the optimum values for each parameter.

card_number

Specifies the number of the card for which to display information. If no card number is specified, the command displays information for each of the running cards.

Usage

Displays the configuration of the underlying VM hardware for a specific card or all cards in the VPC. When no optional keywords are provided, the command displays information regarding the configured vCPU, memory size, huge page size, crypto hardware and the NIC.

Example

This command displays the hardware configuration associated with card number 1:

```
show cloud hardware test 1
```

This command displays the hardware configuration associated with card number 1:

```
show cloud hardware 1
```

This command displays the optimum hardware configuration for the associated VM hardware:

```
show cloud hardware optimum
```

show cloud monitor

Displays VPC-DI network latency and packet loss statistics for all cards or a specific card in the VPC.

Product

VPC-DI

Privilege

Security Administrator, Administrator, Inspector, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show cloud monitor di-network {detail | summary} card_number
show cloud monitor controlplane [dst dst_slot ] [ src  src_slot ]
show cloud monitor dataplane [dst dst_slot ] [ src  src_slot ]
```

detail

Displays detailed information about the VPC-DI network.

summary

Displays summary information about the VPC-DI network.

card_number

Specifies the number of the card for which to display information.

controlplane

Displays the most recent Control Plane monitor information.

dataplane

Displays the most recent Data Plane monitor information.

dst *dst_slot*

Specifies the slot to which the request was directed.

src *src_slot*

Specifies the slot that originated the request.

Usage Guidelines

Displays the configuration of the underlying VM hardware for a specific card or all cards in the VPC. It provides information regarding the configured vCPU, memory size, huge page size, crypto hardware and the NIC.

The **show cloud monitor controlplane [dst** *dst_slot* **] [src** *src_slot* **]** command displays the most recent Control Plane monitor information.

The **show cloud monitor dataplane [dst** *dst_slot* **] [src** *src_slot* **]** command displays the most recent Control Plane monitor information.

Example

This command displays summary monitored statistics for VPC-DI network communications from and to the third card in the VPC. The display shows the test packet loss rate for the past five minutes and past 60 minutes. If the rate is larger than 1%, the health status is marked as "Bad".

```
show cloud monitor di-network summary 3
```

```
Card 3 Test Results:

ToCard   Health   5MinLoss   60MinLoss
   1      Good       0.0%       0.0%
   2      Good       0.0%       0.0%
   4       Bad       6.32%      5.36%
   5      Good       0.0%       0.0%
   6      Good       0.0%       0.0%
```

The following command displays slot 3 as the source slot from where the Control Plane monitor information originated.

Specifies the slot that originated the request.

```
show cloud monitor controlplane src_slot 3
```

The following command displays slot 6 as the destination slot from where the most recent Data Plane monitor information was requested.

```
show cloud monitor dataplane dst_slot 6
```

show cmp history

Displays historical information for the last 100 Certificate Management Protocol v2 transactions.

Product

All products supporting IPSec CMPv2 features

Important This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege Security Administrator

Command Modes Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description **`show cmp history`**

Usage Guidelines Display historical information for the last 100 Certificate Management Protocol v2 transactions.

Example

The following command displays CMPv2 transaction history:

`show cmp history`

show cmp outstanding-req

Displays details regarding outstanding Certificate Management Protocol v2 requests.

Product All products supporting IPSec CMPv2 features

Important This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege Security Administrator

Command Modes Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description **`show cmp outstanding-req`**

Usage Guidelines Display information for outstanding Certificate Management Protocol v2 requests.

Example

The following command displays outstanding CMPv2 requests:

`show cmp outstanding-req`

show cmp statistics

Displays statistics related to Certificate Management Protocol v2 functions.

Product

All products supporting IPSec CMPv2 features

Important

This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege

Security Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show cmp statistics`

Usage Guidelines

Display statistics related to Certificate Management Protocol v2 functions.

Example

The following command displays CMPv2 statistics:

`show cmp statistics`

show confdmgr

Displays information about the StarOS ConfD Manager (confdmgr) process and its association with NETCONF protocol. ConfD and NETCONF intercommunicate with the Cisco Network Service Orchestrator (NSO).

Product

All

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax

`show confdmgr [ confd { cdb | netconf | state } | model { bulkstats | confd } | subscriptions ] [ | { grep` *`grep_options`* **`| more } ]`**

confd { cdb | netconf | state }

Displays information about the ConfD engine based on the specified keyword:

- **cdb** - displays ConfD Configuration Database (CDB) information
- **netconf** - displays NETCONF state information
- **state** - displays current ConfD state information

model { bulkstats | confd }

Displays information about the ConfD model based on the specified keyword:

- **bulkstats** - bulk statistics configuration and operational data
- **confd** - server ConfD configuration

subscriptions

Displays ConfD CDB subscription information.

| { 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.

Usage Guidelines

Used this command to display useful in monitoring and troubleshooting NETCONF protocol.

Example

The following command displays ConfD subscription information.

```
show confdmgr subscriptions
```

show configuration

Displays current configuration information for various subcomponents of the system.

Product

All

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show configuration [active-charging service { all | name *srvc_name* **} | apn** *apn_name*

| brief | bulkstats | card *card_num* **| checksum | context** *name* **| link-aggegation group** *group_number* **| obsolete-encryption | port** *slot/port* **| rohc | showsecrets | srp | url** *url* **| verbose] [| { grep** *grep_options* **| more }]**

show configuration active-charging service { all | name *srvc_name* **} [brief | obsolete-encryption | showsecrets | verbose]**
show configuration apn *apn_name* **[obsolete-encryption | showsecrets | verbose]**
show configuration brief
show configuration bulkstats [brief | verbose]
show configuration card *card_num* **[brief | obsolete-encryption | showsecrets | verbose]**
show configuration checksum [brief | obsolete-encryption | showsecrets | verbose]
show configuration confd [brief | verbose]
show configuration context *name* **[brief | obsolete-encryption | radius | showsecrets | verbose]**
show configuration link-aggregation group *group_number*
show configuration obsolete-encryption
show configuration port *slot/port* **[brief | obsolete-encryption | showsecrets | verbose]**
show configuration rohc [all | profile-name *name* **] [brief | verbose]**
show configuration showsecrets [obsolete-encryption]
show configuration srp [brief | checksum | obsolete-encrpytion | showsecrets | verbose]
show configuration url *url*
show configuration verbose [obsolete-encrpytion | showsecrets]

active-charging service { all | name *srvc_name* | statistics}

Displays all active charging parameters for all services, or a specified service name expressed as an alphanumeric string of 1 through 15 characters, or service statistics.

apn *apn_name*

Specifies an APN for which to display the configuration information. All contexts are searched for this APN, and if a match found, the StarOS returns the configuration of this APN.

brief

Displays current configuration information in brief form.

Important The **brief** keyword is only available in StarOS 20.0 and higher releases.

bulkstats

Displays the URL for the backup bulkstats configuration file if it has been configured.

card *card_num*

Specifies a card for which configuration information is to be displayed as an integer from 1 through 48 for the ASR 5000 or 1 through 20 for the ASR 5500.

checksum

Generates and displays a checksum value for the configuration data.

confd

Displays subset of configuration information for ConfD and NETCONF protocol. (ASR 5500 and VPC platforms only)

context *name*

Specifies an existing context for which configuration information is to be displayed as an alphanumeric string of 1 through 79 characters.

link-aggregation group *group_number*

Displays the current configuration of the LAG specified by group number as an integer from 1 through 1023.

obsolete-encryption

Shows encrypted values using a weaker, obsolete encryption method (prior to release 12.2).

Important The **obsolete-encryption** keyword is only available in StarOS 19.1 and prior releases.

port *slot/port*

Displays configuration information for a port identified by its slot and port numbers.

rohc [all | profile-name *name*

Specifies that information for all robust header compression (RoHC) profiles or the named profile is to be displayed.

showsecrets

Displays encrypted and unencrypted secret keys saved in the configuration. If this keyword is not specified, secret keys are not displayed.

Important This keyword is restricted to Administrator privilege or higher.

Important The **showsecrets** keyword is only available in StarOS 19.1 and prior releases.

srp

Shows the Service Redundancy Protocol (SRP) configuration used for Interchassis Session Recovery (ICSR) deployments.

url *url*

Default: configuration which is currently in use.

This keyword is not available to users with Operator level permissions. Specifies the location of the configuration data to use for information display. The *url* may refer to a local or a remote file and must be entered in the following format:

For the ASR 5000:

[file:]{ /flash | /pcmcia1 | /hd }[/*directory* **]/***file_name*
tftp://{ *host***[** *:port#* **] }[/***directory* **]/***file_name*
[http: | ftp: | sftp:]//[*username***[** *:password* **]@] {** *host* **}[** *:port#* **][/***directory* **]/***file_name*

For the ASR 5500:

[file:]{ /flash | /usb1 | /hd }[/*directory* **]/***file_name*
tftp://{ *host***[** *:port#* **] }[/***directory* **]/***file_name*
[http: | ftp: | sftp:]//[*username***[** *:password* **]@] {** *host* **}[** *:port#* **][/***directory* **]/***file_name*

Important FTP is not supported in StarOS 20.0 or higher Trusted Builds.

Important Do not use the following characters when entering a string for the field names below: "/" (forward slash), ":" (colon) or "@" (at sign).

directory is the directory name.

filename is the actual file of interest.

Important Configuration files should be named with a **.cfg** extension.

username is the user to be authenticated.

password is the password to use for authentication.

host is the IP address or host name of the server.

port# is the logical port number that the communication protocol is to use.

verbose

Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

| { 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.

Usage Guidelines

View the current configuration to analyze recent changes. For additional information, refer to the Administration Guides for products installed on your system.

Example

The following command displays the local in-use port configuration information for port *24/1* in verbose mode.

```
show configuration port 24/1 verbose
```

The following command displays the local in-use port configuration information for port *5/11* in verbose mode.

```
show configuration port 5/11 verbose
```

The following command displays the configuration of all RADIUS server groups configured in context *local*

```
show configuration context local radius group all
```

The following command shows the configuration for a context named PGW.

```
show configuration context pgw
```

show configuration errors

Displays current configuration errors and warning information for the target configuration file as specified for a service.

Product

All

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show configuration errors [section *section_name* **] [verbose] [| { grep** *grep_options* **| more }]**

section {*section_name*}

Specifies the services and section for which to display and validate a configuration.

The following services and sections are supported:

- **aaa-config**: Displays configuration errors/warnings for the AAA service(s) configured on the system.
- **active-charging**: Displays configuration errors/warnings for the Enhanced Charging Service(s) and the Personal Stateful Firewall service(s) configured on the system.
- **alcap-service**: Displays configuration errors/warnings for Access Link Control Application Part (ALCAP) on HNB-GW for IuCS-over-ATM support towards CS core network.

Important In Release 20 and later, HNBGW is not supported. This keyword must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

- **apn**: Displays configuration errors/warnings for the APN configuration(s) on the system.
- **apn-profile**: Displays configuration errors/warnings for the APN Profile configuration(s) on the system.
- **apn-remap-table**: Displays configuration errors/warnings for the APN Remap Table configuration(s) on the system.
- **asngw-service**: Displays configuration errors/warnings for the Access Service Network Gateway (ASN-GW) Service configured in a specific context for which configuration errors/warnings is to be displayed.
- **asnpc-service**: Displays configuration errors/warnings for the ASN Paging Controller and Location Registry (ASN PC-LR) Service(s) configured on the system.
- **call-control-profile**: Displays configuration errors/warnings for the Call Control Profile configuration(s) on the system.
- **camel-service**: Displays configuration errors/warnings for the Customised Applications for Mobile networks Enhanced Logic (CAMEL) Service configuration(s) on the system.
- **closed-rp-service**: Displays configuration errors/warnings for the closed RP service(s) configured on the system.
- **cs-network**: Displays configuration errors/warnings for the circuit switched (CS) network configuration(s) on the system.
- **diameter**: Displays configuration errors/warnings for the Diameter configuration(s) on the system.
- **dns-client**: Displays configuration errors/warnings for the DNS client configuration(s) on the system.
- **egtp-service**: Displays configuration errors/warnings for the evolved GPRS Tunneling Protocol (eGTP) service configuration(s) on the system.
- **event-notif**: Displays configuration errors/warnings for the event notification (SNMP) interface client.
- **fa-service**: Displays configuration errors/warnings for the Foreign Agent (FA) service(s) configured on the system.
- **fng-service**: Displays configuration errors/warnings for the Femto Network Gateway (FNG) configuration(s) on the system.
- **ggsn-service**: Displays configuration errors/warnings for the Gateway GPRS Support Node (GGSN) service(s) configured on the system.
- **gprs-service**: Displays configuration errors/warnings for the General Packet Radio Service (GPRS) service(s) configured on the system.
- **gs-service**: Displays configuration errors/warnings for the Gs service(s) configured on the system. The Gs interface between the SGSN and the MSC (VLR) uses the BSSAP+ protocol.
- **ha-service**: Displays configuration errors/warnings for the Home Agent (HA) service(s) configured on the system.
- **henbgw-network-service**: Displays configuration errors/warnings for the Home Evolved Node B Gateway (HNB-GW) network service configuration(s) on the system.

Important In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

- **hnbgw-service**: Displays configuration errors/warnings for the Home Evolved Node B Gateway (HNB-GW) Service configuration(s) on the system.

Important In Release 20 and later, HNBGW is not supported. This keyword must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

- **hsgw-service**: Displays configuration errors/warnings for the HRPD Serving Gateway (HSGW) service(s) configured on the system.
- **imei-profile**: Displays configuration errors/warnings for the International Mobile Equipment Identity (IMEI) Profile configuration(s) on the system.
- **imsa-config**: Displays configuration errors/warnings for the IMS Authorization (IMSA) configuration(s) on the system.

Important In 16.0 and later releases, error message will be displayed in the output of **show configuration errors** command when the user tries to configure an endpoint which is already configured in other IMSA service.

- **imssh-service**: Displays configuration errors/warnings for the IMS Sh (IMSSh) service(s) configured on the system.
- **imsue-service**: Displays configuration errors/warnings for the IMS UE service(s) configured on the system.
- **ipms**: Displays configuration errors/warnings for the Intelligent Packet Monitoring System (IPMS) service(s) configured on the system.
- **ipne**: Displays configuration errors/warnings for the IP Network Enabler (IPNE) facility configured on the system.
- **ipsg-service**: Displays configuration errors/warnings for the IP Security Gateway (IPSG) service(s) configured on the system.
- **iups-service**: Displays configuration errors/warnings for the IuPS service(s) configured on the system.
- **lac-service**: Displays configuration errors/warnings for the Layer 2 Tunneling Protocol (L2TP) Access Concentrator (LAC) service(s) configured on the system.
- **lns-service**: Displays configuration errors/warnings for the L2TP Network Server (LNS) service(s) configured on the system.
- **local-policy**: Displays configuration errors/warnings for the Local Policy configuration(s) on the system.
- **map-service**: Displays configuration errors/warnings for the SS7 Mobile Application Part (MAP) service(s) configured on the system.
- **mme-service**: Specifies the configuration errors for a Mobility Management Entity (MME) service configured in a specific context for which configuration errors/warnings are to be displayed.

- **operator-policy**: Displays configuration errors/warnings for the Operator Policy configuration(s) on the system.
- **pcc-policy-service**: Displays configuration errors/warnings for the Policy and Charging Control (PCC) Policy Service configuration(s) on the system.
- **pcc-quota-service**: Displays configuration errors/warnings for the Policy and Charging Control (PCC) Quote Service configuration(s) on the system.
- **pcc-service**: Displays configuration errors/warnings for the PCC Service configuration(s) on the system.
- **pdg-service**: Displays configuration errors/warnings for the Packet Data Gateway (PDG) Service configuration(s) on the system.
- **pdif-service**: Displays configuration errors/warnings for the Packet Data Interworking Function (PDIF) service(s) configured on the system.
- **pdsn-service**: Displays configuration errors/warnings for the Packet Data Serving Node (PDSN) service(s) configured on the system.
- **pgw-service**: Displays configuration errors/warnings for the PDN-Gateway (P-GW) service configuration(s) on the system.
- **phsgw-service**: Displays configuration errors/warnings for the Payload Header Suppression (PHS) Gateway service(s) configured on the system.
- **policy-grp-config**: Displays configuration errors/warnings for the Policy Group configuration(s) on the system.
- **ps-network**: Displays configuration errors/warnings for the packet switched (PS) network configuration(s) on the system.
- **saegw-service**: Displays configuration errors/warnings for the System Architecture Evolution Gateway (SAE-GW) Service configuration(s) on the system.
- **sccp-network**: Displays configuration errors/warnings for the Signaling Connection Control Part (SCCP) network configuration(s) on the system.
- **sgs-service**: Displays configuration errors/warnings for the SGs Service configuration(s) on the system. The SGs interface connects the databases in the VLR and the MME.
- **sgsn-mode**: Displays configuration errors/warnings for the Serving GPRS Support Node (SGSN) mode configuration(s) on the system.
- **sgsn-service**: Displays configuration errors/warnings for the SGSN service(s) configured on the system.
- **sgtp-service**: Displays configuration errors/warnings for the SGSN GPRS Tunneling Protocol (SGTP) service(s) configured on the system.
- **sgw-service**: Displays configuration errors/warnings for the Serving Gateway (S-GW) service configuration(s) on the system.
- **subscriber-config**: Displays configuration errors/warnings for the subscriber configuration(s) on the system.
- **subscriber-map**: Displays configuration errors/warnings for the Subscriber Map configuration(s) on the system.

verbose

Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

| { 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 more information on the usage of **grep** and **more**, refer *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage Guidelines

Use this command to view the current configuration errors and warning to review recent changes. For additional information, refer to the Administration Guides for products installed on your ASR 5x00 system.

Example

The following command displays configuration errors and warnings for all services configured in a context/system:

```
show configuration errors verbose | more
```

The following command displays configuration errors and warnings for Active Charging service and Personal Stateful Firewall service configured in a context:

```
show configuration errors section active-charging verbose
```

The following command displays configuration errors and warnings for QoS-configuration in a context:

```
show configuration errors section qos-marking verbose
```

show congestion-control

Displays information pertaining to congestion control functionality on the system

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

```
show congestion-control { configuration | statistics { manager [ all |
instance task_instance ] } [ | { grep grep_options | more } ]
show congestion-control statistics mme { critical | full | major | minor
 } [ | { grep grep_options | more } ]
```

configuration

Displays congestion control configuration information including threshold parameters and policy settings for the configured services.

statistics

Displays congestion control statistics for manager services.

manager

Specifies the name of the service/session manager for which statistics are displayed. The following types of *manager* services are supported:

- **a11mgr**: Specifies that statistics are displayed for PDSN services.
- **asngwmgr**: Specifies that statistics are displayed for ASN-GW services.

Important ASNGW is no longer supported. For more information, contact your Cisco account representative.

- **asnpcmgr**: Specifies that statistics are displayed for ASN PC-LR services.
- **bindmux**: Specifies that statistics are displayed for Bindmux Manager used by PCC service.
- **egtpinmgr**: Specifies that statistics are displayed for EGTP ingress demuxmgr.
- **gtpcmgr**: Specifies that statistics are displayed for GGSN services.
- **hamgr**: Specifies that statistics are displayed for HA services.
- **hnbmgr**: Specifies that statistics are displayed for HNB Manager used by HNB-GW service.

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- **imsimgr**: Specifies that statistics are displayed for IMSI managers.
- **ipsecmgr**: Specifies that statistics are displayed for IPSec managers.
- **ipsgmgr**: Specifies that statistics are displayed for IPSG managers.
- **l2tpmgr**: Specifies that statistics are displayed for L2TP managers.
- **service**: Specifics that statistics are displayed for services.
- **sgmbmgr**: Specifies that statistics are displayed for SGMB Demux managers.

statistics mme { critical | full | major | minor }

Displays the statistics based on the current state of all instances of the specified task.

- **critical**: Specifies that statistics are displayed for the critical congestion policy for MME services.
- **full**: Specifies that statistics are displayed for all congestion policies for MME services.
- **major**: Specifies that statistics are displayed for the major congestion policy for MME services.
- **minor**: Specifies that statistics are displayed for the minor congestion policy for MME services.

all

Displays the statistics based on the current state of all instances of the specified task.

instance *task_instance*

Displays statistics for a specified software task instance. *task_instance* can be configured to an integer from 1 to 128.

Important The **inst** column of the **show task table** command output displays the instance of a particular task.

| { 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.

Usage Guidelines

This command displays congestion control configuration information or statistics for a particular service type.

When the all keyword is used, the system compares the current state of all instances of the specified task. The state is based on whether or not any congestion control thresholds have been exceeded. If one or more instances are experiencing congestion, the state is displayed as "Applied", and the various thresholds that have been crossed are indicated.

Example

The following command displays congestion control statistics for a PDSN service using an **a11mgr** task with an instance of *2*:

```
show congestion-control statistics a11mgr instance 2
```

The following command displays congestion control statistics for an ASN-GW service using an **asngwmgr** task with an instance of *2*:

```
show congestion-control statistics asngwmgr instance 2
```

The following command displays congestion control statistics for an ASN PC-LR service using an **asnpcmgr** task with an instance of *2*:

```
show congestion-control statistics asnpcmgr instance 2
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show connectedapps

Displays information about the current Connected Apps (CA) configuration.

Product

SecGW (WSG)

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description `show connectedapps`

Usage Guidelines Displays information about the current Connected Apps (CA) configuration between the CA client on the ASR 9000 VSM and IOS-XR.

Example

This command displays Connected Apps configuration information:

```
show connected apps
```

show content-filtering category database

Displays details of the specified category based content filtering database for content filtering application configured in a system/service.

Product CF

Privilege Security Administrator, Administrator, Operator, Inspector

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description **show content-filtering category database [active | all | facility srdbmgr { all | instance** *instance_number* **} | url** *url_string* **] [verbose] [| { grep** *grep_options* **| more }]**

active

Displays the information about all active databases, for example databases in memory. This is the default setting for category database information.

all

Displays the information about all active databases, for example, databases in memory and all saved databases on a system.

facility

Displays logged events for a specific facility.

srdbmgr { all | instance *instance_number* }

Displays logged events for all static rating database managers or for all or for a specific instance.

- **all**: Displays the logged events for all Static Rating Database (SRDB) Manager instances.
- **instance** *instance_number*: Displays events logged for a specific SRDB Manager instance specified as an integer from 1 through 8.

url *url_string*

Displays the information of the database located at the URL that specifies the name/location of the category database from which to retrieve information as an alphanumeric string of 1 through 512 characters.

verbose

This option enables the detailed mode for additional information display for specific database.

| { grep *grep_options* | more }

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

Usage Guidelines

Use this command to display information of database for category based content filtering application in a service.

Example

The following command displays a detailed information for all active databases in memory.

```
show content-filtering category database active all
```

The following command displays the CF database status of all running SRDB managers.

```
show content-filtering category database facility srdbmgr all
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show content-filtering category policy-id

Displays Content Filtering category policy definitions.

Important In StarOS 8.1 and later releases this command is replaced by the **show active-charging content-filtering category policy-id** command.

Product

CF

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show content-filtering category policy-id { all | id *cf_policy_id* **} [| { grep** *grep_options* **| more }]**

all

Displays definitions of all Content Filtering category policies.

id *cf_policy_id*

Displays definitions of an existing Content Filtering category policy ID specified as an integer from 1 through 4294967295.

| { grep *grep_options* | more }

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

Usage Guidelines

Use this command to view Content-Filtering Category definitions for a specific/all Policy IDs.

Example

The following command displays Content Filtering category definitions for policy ID *3*:

```
show content-filtering category policy-id id 3
```

Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

show content-filtering category statistics

Displays statistics for the category-based Content Filtering application configured in a system/service.

Product

CF

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show content-filtering category statistics [facility srdbmgr { all | instance *instance_number* **}] [| { grep** *grep_options* **| more }]**

facility

Displays logged events for a specific facility.

srdbmgr { all | instance *instance_number* }

Displays logged events for all Static Rating Database (SRDB) Manager instances or for the specified instance.

- **all**: Displays events logged for all SRDB Manager instances.
- **instance** *instance_number*: Displays events logged for the SRDB Manager instance specified as an integer from 1 through 8.

| { grep *grep_options* | more }

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

Usage Guidelines

Use this command to view the statistics of Category Based Content Filtering application in a service. This command's output also indicates capability of the system to perform Content Filtering and Dynamic Content Filtering if configured.

Important Content filtering cannot be performed if less than two PSCs are activated. Dynamic Content Filtering cannot be performed if less than three PSCs are activated.

Example

The following command displays the detailed statistics of configured category based content filtering application:

```
show content-filtering category statistics
```

The following command displays the detailed statistics of configured category based content filtering application based on running SRDB Manager *instance1*.

```
show content-filtering category statistics facility srdbmgr instance
instance1
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show content-filtering category url

Displays the information about the categories of the database at the specific URL configured for the category-based content filtering application in a system/service.

Product

CF

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

show content-filtering category url *url_string* **[policy-id** *cf_policy_id* **| rulebase** *rulebase_name* **] [verbose] [| { grep** *grep_options* **| more }]**

url *url_string*

Displays the category information of the URL specified as an alphanumeric string of 1 through 512 characters.

policy-id *cf_policy_id*

Displays the category information of a URL configured with an existing content filtering category policy ID specified as n integer from 0 through 65535.

rulebase *rulebase_name*

Displays the category information of a URL configured in ACS Configuration Mode for category-based content filtering in specific rulebase.

rulebase_name must be the name of an existing rulebase, and must be an alphanumeric string of 1 through 15 characters.

verbose

Enables the detailed mode for additional information display for a specific database.

| { grep *grep_options* | more }

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

Usage Guidelines

Use this command to display information of a database URL for category based content filtering application in a service.

Example

The following command displays a detailed information for all active databases in memory.

```
show content-filtering category url /cf_server/cf/optcmd.bin verbose
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show content-filtering server-group

Displays information for Content Filtering Server Group (CFSG) configured in the service.

Product

CF

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show content-filtering server-group [ name` *`cfsg_name`* **`| statistics ] [ | { grep`** *`grep_options`* **`| more } ]`**

name *cfsg_name*

Displays information for an existing CFSG specified as an alphanumeric string of 1 through 63 characters.

statistics

Displays statistical information for all configured CFSGs.

| { grep *grep_options* | more }

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

Usage Guidelines

Use this command to display information for Content Filtering Server Group configured in a service.

Example

The following command displays a detailed information for all charging actions:

```
show content-filtering server-group statistics
```

The following command displays a details of a specific charging action:

```
show content-filtering server-group name test123
```

Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

show context

Displays information for currently configured contexts.

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

`show context [ all | name` *`context_name`* **`] [ | { grep`** *`grep_options`* **`| more } ]`**

all | name *context_name*

all: Displays information for all currently configured contexts.

name *context_name*: Displays information for an existing context specified as an alphanumeric string of 1 through 79 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.

Usage Guidelines

View configured contexts. This may be useful in verifying configuration or troubleshooting the system.

Example

The following command displays information for the configured context named *sampleContext*:

```
show context name sampleContext
```

The following command displays information for all contexts:

```
show context all
```

Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

show cpu

Displays information on system CPUs.

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

`show cpu { info [ card` *`card_num`* **`[ cpu`** *`cpu_num`* **`] ] [ crypto-cores ] [ graphs ] [ verbose ] | table } [ | { grep`** *`grep_options`* **| more }]`**

info [card *card_num* [cpu *cpu_num*]] [crypto-cores] [graphs] [verbose]

Displays information for an entire card or a specific CPU.

card *card_num*: Specifies the card for which to display associated information. *card_num* must be a value in the range 1 through 48 on the ASR 5000 or 1 through 20 on the ASR 5500 and must refer to an installed card.

cpu *cpu_num*: Optionally selects a specific CPU on the card of interest to display specific information. *cpu_num* must be a value in the range 0 through 3 and must refer to an installed CPU.

The output of **show cpu info card** *n* **verbose** also includes usage details for individual cores within each CPU.

crypto-cores : Optionally, specifies to display the CPU crypto core utilization information.

graphs: In addition to textual CPU information display CPU utilization information in graphs.

verbose: Output is to display all information available.

table

Display, in tabular format, all cards and CPUs.

| { 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.

Usage Guidelines

View CPU statistics to aid in diagnosing service problems for the case of overload conditions.

Important This command is not supported on all platforms.

Example

The following command displays the CPU information in tabular format for all CPUs on all installed cards:

`show cpu table`

The following command displays CPU information for card *8* in verbose mode:

show cpu info card 8 verbose

The following command displays information for CPU *0* on card *1*:

show cpu info card 1 cpu 0

The following command displays information for crypto core utilization for CPU **0** on card **2**:

show cpu info card 2 cpu 0 crypto-cores

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show crash

Displays software crash events records and associated dump files (minicore, NPU or kernel) for all crashes or a specified crash event.

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

show crash

all | list | number *crash_num*

all: Displays the dump files for all crash event records in the crash log.

list: Displays a list of recent crash event records. this is the contents of the crashlog2 file.

number *crash_num* displays the dump file for an existing crash number. The crash number can be displayed using the **list** keyword.

| { 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.

Usage Guidelines

VIew the crash list to determine frequency of crashes or if crashes occur at some specific time of day. To aid in troubleshooting, this command may also be used to view the dump file for a specific crash.

For additional information refer to the *System Logs* section of the *System Administration Guide*.

Example

The following displays the list of crash event records on the active management card.

```
show crash list
```

The following command will display the dump file for crash number *11*.

```
show crash number 11
```

show credit-control sessions

Displays credit control sessions information.

Product

PDSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

`show credit-control session [ all | callid | full | mdn | nai | summary ] [ | { grep` *`grep_options`* **`| more } ]`

session [all | callid | full | mdn | nai | summary]

Displays the credit control session status based on the following keywords:

all: Displays all available information for Credit Control sessions

callid: Displays the Credit Control Session Call ID

full: Displays All available information for the associated display or the filter keyword

mdn: Displays the Credit Control Message Delivery Notification (MDN) information.

nai: Displays the Credit Control NI

summary: Displays the summary of Credit Control session information

| { 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.

Refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

Usage Guidelines

Use this command to show active credit control application for service sessions.

Example

The following command shows the configured Credit Control application sessions:

```
show credit-control sessions
```

show credit-control statistics

Displays credit control statistics.

Product

PDSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show credit-control statistics cc-service *name* **[| { grep** *grep_options* **| more }]**

cc-service

Specifies the Credit Control Service.

name must be the name of a Credit Control Service, and must be 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.

Refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

Usage Guidelines

Use this command to show active credit control statistics.

Example

The following command shows the configured credit control statistics for a service named *service1*:

```
show credit-control statistics cc-service service1
```

show crypto blockedlist file

Displays the contents of the blockedlist (access denied) file.

Product

All products supporting IPSec blockedlist

Privilege

Security 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:

show crypto blacklist file

From StarOS 21.26 and later releases:

show crypto blockedlist file

Usage Guidelines

Use this command to display the current contents of the blockedlist file.

Example

In releases prior to StarOS 21.26:

The following command displays the contents of the blacklist file:

show crypto blacklist file

show crypto group

Displays information pertaining to configured crypto groups.

Important

HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show crypto group [ name` *`group_name`* **`| summary ]`**

name *group_name*

Displays information for an existing crypto group specified as an alphanumeric string of 1 through 127 characters.

summary

Displays state and statistical information for configured crypto groups in this context.

Usage Guidelines

Use this command to display information and statistics pertaining to one or all configured crypto groups within the current context.

If the **summary** keyword is not used, detailed information is displayed.

Example

The following command displays detailed information for a crypto group called *group1*:

`show crypto group name group1`

show crypto ikev1

Displays pre-shared key information for peer security gateways configured within the context.

Important

HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show crypto ikev1 { keys | policy [ preference ] | security-associations [ summary ] }`

keys

Displays the IKE pre-shared key information based on the peer security gateway.

policy [*preference*]

Displays configuration information for the Internet Exchange Key (IKE) policy priority specified as an integer from 1 through 100. If no preference is specified, information will be displayed for all configured policies.

security-associations [summary]

Displays information for established IPSec security associations (SAs).

Usage Guidelines

Use this command to:

- Display pre-shared key information. This information can be used to verify configuration and/or for troubleshooting.
- Verify the configuration of IKE policies within the context.
- Display established IPSec SA information. This information can be used for troubleshooting.

Example

The following command lists the pre-shared keys received from peer security gateways as part of the Diffie-Hellman exchange:

```
show crypto ikev1 keys
```

The following command displays information for an IKE policy with a preference of *1*:

```
show crypto ikev1 policy 1
```

The following command displays the currently established SAs:

```
show crypto ikev1 security-associations summary
```

show crypto ikev2-ikesa security-associations

Displays a summary view of Internet Key Exchange v2 (IKEv2) IKE Security Associations (IKE SAs).

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Administrator, Security Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

show crypto ikev2-ikesa security-associations peer *ipv4/v6_address* **[| { grep** *grep_options* **| more }]**
show crypto ikev2-ikesa security-associations summary [cookies] [distribution] | **[dpd] [ipsecmgr instance** *instance_value* **] [natt [remote-gw** *ipv4/v6_address* **] [spi][| { grep** *grep_options* **| more }]**
show crypto ikev2-ikesa security-associations tag *crypto_map* **[| { grep** *grep_options* **| more }]**

peer *ipv4/v6_address*

Specifies the crypto map peer IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

summary

Displays SA summary information only.

This information can be one of the following:

- **cookies**: Display IKE cookies for connections.

  Important: The **cookies** keyword has been deprecated for release 17.0 and above.

- **distribution**: Display summary distribution.
- **dpd**: Display DPD (Dead Peer Detection) information for connections.
- **ipsecmgr instance** *instance_value*: Display ipsecmgr instance information. *instance_value* is an integer from 177 through 352.
- **natt** [**[remote-gw** *ipv4/v6_address* **]**: Display NAT-T information for connections or a specified remote gateway.
- **spi**: Display IKE Security Parameter Index.

tag *tag_name*

Specifies a crypto map name as an alphanumeric string of 1 through 127 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.

Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

Usage Guidelines

Shows the information of the of the SAs configured for a crypto template. It shows the total configured SA lifetime in seconds and the number of seconds left on the timer.

Example

Use this command to display the SA summary:

```
show crypto ikev2-ikesa security-associations summary
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show crypto ikev2-ikesa transform-set

Displays IKEv2/IKESA (Internet Key Exchange v2/IKE Security Association) transform set configuration information.

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show crypto ikev2-ikesa transform-set *transform_set_name* [**|** { **grep** *grep_options* | **more** }

show crypto ikev2-ikesa transform-set *transform_set_name*

Specifies the name of an existing IKEv2/IKSA transform set for which to display information as an alphanumeric string of 1 through 127 characters that is case sensitive.

|{ 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.

Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

Usage Guidelines

Use this command to verify the configuration of IKEv2/IKESA transform sets within the context.

If no keyword is specified, information will be displayed for all IKEv2/IKESA transform sets configured within the context.

Example

The following command displays information for an IKEv2/IKESA transform set named *test1*:

```
show crypto ikev2-ikesa transform-set test1
```

show crypto ipsec security-associations

Displays IPSec security associations (SAs) configured within or facilitated by the context and can optionally display statistics for them.

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show crypto ipsec security-associations` `[` **`map-type`** `{` **`ikev2-ipv4-cfg`** | **`ikev2-ipv4-node`** | **`ikev2-ipv6-cfg`** | **`ikev2-ipv6-node`** | **`ipsec-dynamic`** | **`ipsec-ikev1 | ipsec-ikev2-subscriber`** | **`ipsec-l2tp`** | **`ipsec-manual`** | **`ipsec-mobile-ip`** `}` | **`summary`** `[` **`distribution`** | **`ipsecmgr`** | **`map-type`** `]` | `[` **`|`** `{` **`grep`** *`grep_options`* | **`more`** `}` `]` | `[` **`tag`** *`tag_name`* `]` | `[` **`|`**`{` **`grep`** *`grep_options`* | **`more`** `}` `]`

map-type { ikev2-ipv4-cfg | ikev2-ipv4-node | ikev2-ipv6-cfg | ikev2-ipv6-node | ipsec-dynamic | ipsec-ikev1 | ipsec-ikev2-subscriber | ipsec-l2tp | ipsec-manual | ipsec-mobile-ip }

Specifies that information for all crypto maps of a specific type configured within the context will be displayed. The following types can be specified:

- **ikev2-ipv4-cfg**: IKEv2 IPv4 IPSec configured (ACL) Tunnel
- **ikev2-ipv4-node**: IKEv2 IPv4 IPSec spawned node Tunnel
- **ikev2-ipv6-cfg**: IKEv2 IPv6 IPSec configured (ACL) Tunnel
- **ikev2-ipv6-node**: IKEv2 IPv6 IPSec spawned node Tunnel
- **ipsec-dynamic**: Dynamic IPSec Tunnel
- **ipsec-ikev1**: IKEv1 IPSec Tunnel
- **ipsec-ikev2-subscriber**: IKEv2 Subscriber Tunnel
- **ipsec-l2tp**: L2TP IPSec Tunnel
- **ipsec-manual**: Manual (Static) IPSec Tunnel
- **ipsec-mobile-ip**: Mobile IP IPSec Tunnel

summary [distribution | ipsecmgr | map-type]

Displays only security association summary information.

distribution: Show IPSec Manager SA distribution information.

ipsecmgr *ipsec_mgr_id*: Displays summary SA information for the IPSec manager instance ID specified as an integer from 1 through 200.

map-type *map_type*: Displays summary SA information for the specified type of crypto map.The following types can be specified:

- **ikev2-ipv4-cfg**: IKEv2 IPv4 IPSec configured (ACL) Tunnel
- **ikev2-ipv4-node**: IKEv2 IPv4 IPSec spawned node Tunnel
- **ikev2-ipv6-cfg**: IKEv2 IPv6 IPSec configured (ACL) Tunnel
- **ikev2-ipv6-node**: IKEv2 IPv6 IPSec spawned node Tunnel
- **ipsec-dynamic**: Dynamic IPSec Tunnel
- **ipsec-ikev1**: IKEv1 IPSec Tunnel
- **ipsec-ikev2-subscriber**: IKEv2 Subscriber Tunnel
- **ipsec-l2tp**: L2TP IPSec Tunnel
- **ipsec-manual**: Manual (Static) IPSec Tunnel
- **ipsec-mobile-ip**: Mobile IP IPSec Tunnel

tag *tag_name*

Displays the SAs for an existing crypto map specified as an alphanumeric string of 1 through 127 characters that is case sensitive.

|{ 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.

Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

Usage Guidelines

Use this command to display IPSec SA information and statistics. This information can be used for performance monitoring and/or troubleshooting.

The displayed information categorizes control signal and data statistics. Data statistics are further categorized according to the encapsulation method, either GRE or IP-in-IP.

Example

The following command displays summary SA statistics for all IPSec managers.

```
show crypto ipsec security-associations summary
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show crypto ipsec transform-set

Displays IPSec transform set configuration information.

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show crypto ipsec transform-set [` *`transform_name`* **`]`**

transform_name

Displays information for the IPSec transform set specified as an alphanumeric string of 1 through 127 characters that is case sensitive.

Usage Guidelines

Use this command to verify the configuration of IPSec transform sets within the context.

If no keyword is specified, information will be displayed for all IPSec transform sets configured within the context.

Important This command is supported in PDIF Release 8.3 only.

Example

The following command displays information for an IPSec transform set named *test1*:

```
show crypto ipsec transform-set test1
```

show crypto isakmp keys

Displays pre-shared key information (Internet Security Association and Key Management Protocol, ISAKMP) for peer security gateways configured within the context.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show crypto isakmp keys
```

Usage Guidelines

Use this command to display pre-shared key information based on the peer security gateway. This information can be used to verify configuration and/or for troubleshooting.

Example

The following command lists the pre-shared keys received from peer security gateways as part of the Diffie-Hellman exchange:

```
show crypto isakmp keys
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show crypto isakmp policy

Displays Internet Security Association and Key Management Protocol (ISAKMP) policy configuration information.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show crypto isakmp policy [ preference ]`

preference

Displays configuration information for the ISAKMP policy priority specified as an integer from 1 through 100.

Usage Guidelines

Use this command to verify the configuration of ISAKMP policies within the context.

If no *preference* is specified, information will be displayed for all configured policies.

Example

The following command displays information for an ISAKMP policy with a preference of *1*:

`show crypto isakmp policy 1`

show crypto isakmp security-associations

Displays currently established Internet key Exchange (IKE) security associations (SAs) facilitated by the context.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show crypto isakmp security-associations [ cookies ]`

cookies

Specifies that cookies should be displayed.

Usage Guidelines

Use this command to display established IPSec SA information. This information can be used for troubleshooting.

Example

The following command displays the currently established SAs:

```
show crypto isakmp security-associations
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show crypto managers

Displays statistics per IPSec Manager.

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

show crypto managers [context *context_name* **| crypto-map** *map_name* **| instance** *instance_num* **| summary [distribution | ike-stats | ikev2-stats | ipsec-sa-stats | npu-stats] | |** { **grep** *grep_options* | **more** }]

context *context_id*

Displays IPSec manager statistics for an existing context specified as n alphanumeric string of 1 through 80 characters.

crypto-map *map_name*

Displays IPSec Managers for an existing crypto map specified as an alphanumeric string of 1 through 128 characters.

instance *instance_num*

Displays statistics for the IPSec manager instance specified as an integer from 1 through 366.

summary [distribution | ike-stats | ikev2-stats [demux-stats] | ipsec-sa-stats | npu-stats]

Shows statistics per service IP address for each manager.

distribution: Displays a summary list of IPSec manager distribution.

ike-stats: Displays a summary list of IPSec IKE statistics. for each IPSec manager.

ikev2-stats: Displays IKEv2 Statistics on each IPSec Manager.

- **demux-stats**: Displays session demux statistics on each IPSec Manager.

ipsec-sa-stats: Displays a summary list of IPSec Security Association (SA) statistics for each IPSec Manager.

npu-stats: Displays NPU statistics on each IPSec Manager.

| { 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.

Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

Usage Guidelines

Use this command to view statistics relating to IPSec managers.

Example

The following command displays summary information for all IPSec managers:

```
show crypto managers summary
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show crypto map

Displays crypto map configuration information.

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show crypto map [**map-type** [**ikev2-ipv4-cfg** | **ikev2-ipv4-node** | **ikev2-ipv6-cfg** | **ikev2-ipv6-node** | **ipsec-ikev1 | ipsec-ikev2-subscriber** | **ipsec-l2tp** | **ipsec-manual** | **ipsec-mobile-ip** | **|** { **grep** *grep_options* | **more** }] | [**summary**] | [**tag** *tag_name*] | [**|**{ **grep** *grep_options* | **more** }]

map-type [ikev2-ipv4-cfg | ikev2-ipv4-node | ikev2-ipv6-cfg | ikev2-ipv6-node | ipsec-ikev1 | ipsec-l2tp | ipsec-manual | ipsec-mobile-ip | | { grep *grep_options* | more }]

Specifies that information for all crypto maps of a specific type configured within the context will be displayed. The following types can be specified:

- **ikev2-ipv4-cfg**: IKEv2 IPv4 IPSec configured (ACL) Tunnel
- **ikev2-ipv4-node**: IKEv2 IPv4 IPSec spawned node Tunnel
- **ikev2-ipv6-cfg**: IKEv2 IPv6 IPSec configured (ACL) Tunnel
- **ikev2-ipv6-node**: IKEv2 IPv6 IPSec spawned node Tunnel
- **ipsec-ikev1**: IKEv1 IPSec Tunnel
- **ipsec-ikev2-subscriber**: IKEv2 Subscriber Tunnel
- **ipsec-l2tp**: L2TP IPSec Tunnel
- **ipsec-manual**: Manual (Static) IPSec Tunnel
- **ipsec-mobile-ip**: Mobile IP IPSec Tunnel

summary

Displays summary information for all crypto maps configured in the context.

tag *map_name*

Specifies the name of an existing crypto map in the current context for which to display configuration information as an alphanumeric string of 1 through 127 characters that is case sensitive.

| { 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.

Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

Usage Guidelines

Use this command to verify the configuration of crypto maps within the context.

If no keyword is specified, information will be displayed for all maps configured within the context regardless of type.

Example

The following command displays configuration information for a dynamic crypto map named *test_map3*:

```
show crypto map tag test_map3
```

show crypto statistics

Displays Internet Protocol Security (IPSec) statistics.

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show crypto statistics` `[` **`ikev1`** `|` **`ikev2`** `[` **`service-ip-address`** *`ip-address`* `]` `[` **`service-name`** *`name`* `]` `|` `[` **`|`** `{` **`grep`** *`grep_options`* `|` **`more`** `]` `]`

ikev1

Displays global ikev1 statistics for this context.

ikev2 [service-ip-address *ip-address*] [service-name *name*]

Displays global ikev2 statistics for this context.

service-ip-address *ip-address*: Specifies the Packet Data Interworking Function (PDIF) service IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

service-name*name*: Specified PDIF service name, a string of size 1 through 63.

| { 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.

Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

Usage Guidelines

Use this command to display statistics for IPSec tunnels facilitated by the context. This information can be used for performance monitoring and/or troubleshooting.

Example

The following command displays cumulative IPSec statistics for the current context:

```
show crypto statistics
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show crypto template

Displays information about crypto templates.

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show crypto template [ map-type [ ikev2-dynamic | ipsec-dynamic ] | summary | tag map_name ] [ | { grep grep_options | more`

map-type [ikev2-dynamic | ipsec-dynamic

Specifies a specific map type.

summary

Displays summary information for all templates.

tag *map_name*

Specifies a crypto map name as an alphanumeric string of 1 through 127 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.

Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

Usage Guidelines

Use this command to display statistics for crypto templates. This information can be used for performance monitoring and/or troubleshooting.

Example

The following command displays summary information for all crypto templates:

```
show crypto template summary
```

show crypto vendor-policy

Displays information about crypto vendor policy.

Product

ePDG

FA

GGSN

HA

HeNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show crypto vendor-policy [ name` *`vendor_policy_name`* **`| summary ] [ | grep`** *`grep_options`* **`| more ]`**

name *vendor_policy_name*

Displays information on the specified vendor policy.

vendor_policy_name must be an alphanumeric string from 1 to 127 characters.

summary

Displays summary information for all vendor policies.

| { 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.

Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

Usage Guidelines

Use this command to display statistics for crypto templates. This information can be used for performance monitoring and/or troubleshooting.

Example

The following command displays summary information for all crypto vendor policies:

```
show crypto vendor-policy summary
```

show crypto permitlist file

Displays the contents of the permitlist (access granted) file.

Product

All products supporting IPSec permitlisting

Important This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege

Security 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:

```
show crypto blacklist file
```

From StarOS 21.26 and later releases:

```
show crypto blockedlist file
```

Usage Guidelines

Use this command to display the current contents of the permitlist file.

Example

In releases prior to StarOS 21.26:

The following command displays the contents of the whitelist file:

```
show crypto whitelist file
```

show cs-network

Important In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Displays statistics for the Circuit Switched (CS)-network(s) instance configured on a chassis for HNB-GW service sessions.

Product

HNB-GW

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show cs-network { all | name` *`cs_name`* **`} [ status ] [ | { grep`** *`grep_options`* **`| more }]`**

all

Displays status counters for all CS (circuit switched) networks configured for HNB-GW service sessions on a chassis.

name *cs_name*

Displays status counters for a CS network configured for HNB-GW service specified as an alphanumeric string of 1 through 127 characters that is case sensitive

| { 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.

Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

Usage Guidelines

Use this command to display the status of any or all CS-network(s) instance configured on a chassis for HNB-GW service sessions.

Example

The following command displays the output for CS network instance status named *cs_1_hnb*:

`show cs-network name cs_1_hnb status`

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show cs-network counters

Important In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Displays the session counter information for an HNB-CS Network associated with Home-NodeB Gateway (HNB-GW) services configured and running on a system.

Product

HNB-GW

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show cs-network counters [name *cs_svc_name* **[msc** *msc_point_code* **]] [| { grep** *grep_options* **| more }]**

name *cs_svc_name*

Filters the counter display based on an existing HNB-CS Network service name associated with an HNB-GW service running on system. *cs_svc_name* is an alphanumeric string of 1 through 63 characters.

msc *msc_point_code*

Filters the counter display filtered on the basis of MSC address provided in the SS7 point code that is connected to a particular HNB-CS Network service. *msc_point_code* must be the address of an MSC in SS7 point code notation.

| { 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 the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in *Command Line Interface Overview* chapter.

Usage Guidelines

Use this command to view the session counter information for HNB-CS Network services configured and MSCs connected on a system.

Example

The following command displays the counters for the HNB-CS Network service named *hnb_cs_svc1*:

```
show cs-network counters name hnb_cs_svc1
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show cs-network statistics

Important In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Displays the Circuit Switched session statistics for Home-NodeB Gateway (HNB-GW) services configured and running on this system.

Product

HNB-GW

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show cs-network statistics [ name` *`cs_svc_name`* **`[ msc`** *`msc_point_code`*`]] [ ranap-only | rtp-only | sccp-only ] [ | { grep`** *`grep_options`* **`| more } ]`**

name *cs_svc_name*

Filters the session statistics display based on an existing HNB-CS Network service name that is associated with an HNB-GW service running on this system. *cs_svc_name* is an alphanumeric string of 1 through 63 characters.

msc *msc_point_code*

Filters the counter display filtered on the basis of MSC address provided in the SS7 point code that is connected to a particular HNB-CS Network service. *msc_point_code* must be the address of an MSC in SS7 point code notation.

ranap-only

Filters the session statistics to display only Radio Access Network Application Protocol (RANAP) traffic for an HNB-CS Network service which is configured and associated with an HNB-GW service running on this system.

rtp-only

Filters the session statistics to display only Realtime Streaming Protocol (RTP) and Realtime Streaming Control Protocol (RTCP) traffic for the specified HNB-CS Network service which is configured and associated with an HNB-GW service running on this system.

sccp-only

Filters the session statistics to display only Signaling Connection Control Part (SCCP) traffic for the specified HNB-CS Network service which is configured and associated with an HNB-GW service running on this system.

| { 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 the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in *Command Line Interface Overview* chapter of the *Command Line Interface Reference*.

Usage Guidelines

Use this command to view the session statistics for overall session or in selected part of user session for HNB-GW services configured and running on this system.

Example

The following command displays the session statistics for RTP and RTCP part of session for the HNB-CS Network service named *hnb_cs1*:

```
show cs-network statistics name hnbcs1 rtp-only
```

Important Output descriptions for commands are available in the *Statistics and Counters Reference*.

show css delivery-sequence

In StarOS 9.0 and later releases, this command is deprecated.

show css server

In StarOS 9.0 and later releases, this command is deprecated.

show css service

In StarOS 9.0 and later releases, this command is deprecated.