Exec Mode show Commands (H-L)

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 ha-service** through **show lte-policy**.

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 ha-service

Displays information on configured Home Agent (HA) services.

Product

HA

Privilege

Security Administrator Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show ha-service { all | name ha_name } [ | { grep grep_options | more } ]
```

all | name *ha_name*

all: Displays information on all Home Agent services.

name *ha_name*: Displays information for an existing HA 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

Display home agent service configuration information.

Example

The following commands displays information on the HA service *sampleService* and all services, respectively.

```
show ha-service name sampleService
```

```
show ha-service all
```

show ha-spi-list

Displays all or a specific Home Agent-Security Parameters Index (HA-SPI) remote address list(s).

Product HA

Privilege Security Administrator Operator, Inspector

Command Modes Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

```
show ha-spi-list { all | name ha_name } [ | { grep grep_options | more } ]
```

all | name *ha_name*

all: Displays information on all HA-SPI lists.

name *ha_name*: Displays information for an existing HA-SPI list 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 Display a single or all HA-SPI lists.

Example

The following commands displays information on the HA-SPI list named *spi012* and all lists, respectively.

```
show ha-spi-list name spi012
```

```
show ha-spi-list all
```

show hardware

Displays information on the system hardware.

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 hardware { card [ card_num ] | inventory | version [ board | diags |
fans] } [ | { grep grep_options | more } ]
```

card [*card_num*]

Provides the hardware information for all ASR 5x00 cards or the card specified by *card_num*. *card_num* must be a value in the range 1 through 48 for the ASR 5000 or 1 through 20 for the ASR 5500 and must refer to an installed card.

inventory

Displays the ASR 5x00 hardware information for all slots in tabular format.

version [board | diags | fans]

Displays the CPU information for all ASR 5x00 application cards and fan controller version for the upper and lower fan trays.

board: Only include the CPLD and FPGA version information.

diags: Only include the CFE diagnostics version information.

fans: Show the fan controller versions for the upper and lower fan trays.

| { 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 hardware information and hardware component versions.

Example

The following displays the hardware information for a card installed in slot *1*.

```
show hardware card 1
```

The following command displays the hardware inventory for the entire chassis.

```
show hardware inventory
```

The following command results in the display of the CPU version for all application cards displaying only the CPLD and FPGA information.

```
show hardware version board
```

The following command displays VPC virtual card information:

```
show hardware
```

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

show hd raid

Shows the output of the Redundant Array of Independent Disks (RAID) established on the ASR 5000 SMCs or ASR 5500 FSCs.

Product

All

Privilege

Security Administrator, Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show hd raid [ verbose ]
```

Example

The following command displays HD RAID configuration information:

```
show hd raid verbose
```

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

show hd-storage-policy

Displays Array Configuration Replicator (ACR) counter and statistical information.

Product

HSGW

P-GW

SAEGW

S-GW

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show hd-storage-policy { all | counters [ all ] [ name name ] [ verbose ]
 | name name | statistics [ all ] [ name name ] [ verbose ] }
```

all

Displays ACR information for all HD storage policies configured on the system.

counters [all] [name *name*] [verbose]

all: Displays ACR counter information for all HD storage policies configured on the system.

name *name*: Displays ACR counter information for an existing HD storage policy specified as an alphanumeric string of 0 through 63 characters.

statistics [all] [name *name*] [verbose]

all: Displays ACR statistical information for all HD storage policies configured on the system.

name *name*: Displays ACR statistical information for an existing HD storage policy specified as an alphanumeric string of 0 through 63 characters.

verbose

Displays HD storage statistics based on instance.

Usage Guidelines

Use this command to display ACR counter and statistic information.

Example

The following command displays ACR statistical information for an HD storage policy named *pgwsgw*:

```
show hd-storage-policy statistics name pgwsgw
```

show henbgw

Important In Release 20, 21.0 and 21.1, HeNBGW is not supported. This command must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

This command displays Home evolved NodeB Gateway (HeNBGW) service related information.

Product

HeNBGW

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show henbgw { henb-association [ all | full | henbgw-access-service
henbgw_acc_svc_name  | peer-address peer_ip_address  | peer-id peer_id_value |
summary ] | session  [ all | callid  call_id | full [ all | callid call_id
| qci qci_value | s1-peer s1_peer_address ] | qci qci_value | s1-peer s1_peer_address
 | summary [ all | callid call_id | qci qci_value | s1-peer s1_peer_address ]
]| ue [ all | summary ] [ | { grep grep_options | more } ] }
```

henb-association [all | full | henbgw-access-service *henbgw_acc_svc_name* | peer-address *peer_ip_address* | peer-id *peer_id_value* | summary]

henb-association : Displays information about HENB associations.

all: Displays information for all HeNB associations.

full: Displays all available information for associated display or filter keyword (previous keyword).

henbgw-access-service: Displays information about HeNB associations with the specified HeNBGW access service.

henbgw_acc_svc_name is an alphanumeric string of 1 through 63 characters.

peer-address: Displays information about HeNB associations with the specified peer.

peer_ip_address is an IPv4 address in dotted-decimal notation or an IPv6 address in colon-separated-hexadecimal notation.

peer-id: Displays information about HeNB associations for the specified peer.

peer_id_value is an integer from 0 to 4294967295.

summary: Displays a summary of available information for the associated keyword (previous keyword).

session

Displays HeNBGW sessions.

all

Displays information for all HeNB sessions.

call-id*call_id*

call-id: Specifies a Call Identification Number. *call_id* is an eight-digit hexadecimal number.

full

Displays information on session state for matching sessions.

qci *qci_value*

call-id: Displays information for the HeNB associated with a specific QCI value. *qci_value* is an integer between 1 and 9.

s1-peer *s1_peer_address*

s1-peer: a specific S1 peer identified by the IP address of a peer eNodeB.

s1_peer_address is an IPv4 address in dotted-decimal notation or an IPv6 address in colon-separated-hexadecimal notation.

summary

This command displays summary information covering matching sessions.

ue

Displays UE 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

Use this command to displays HeNBGW service related information.

Example

The following command displays information for all HeNB associations :

```
show henbgw henb-association all
```

show henbgw-access-service

Important In Release 20, 21.0 and 21.1, HeNBGW is not supported. This command must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

This command displays HeNBGW Access service related information.

Product

HeNBGW

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show henbgw-access-service { all | henb-association [ all | csg-id csg_id_value| full | henbgw-access-service henbgw_acc_svc_name | peer-address peer_ip_address | peer-id peer_id_value | summary | tai mcc mcc_val mnc mnc_val tac ] | name name | statistics [ henbgw-access-service henbgw_acc_svc_name | miscellaneous [ verbose ] | peer-id peer_id_values1ap [ cause | [ verbose ] ] | sctp [ buffer [ sessmgr sessmgr_value] ] [ verbose ] ] [ | { grep grep_options | more } ]}
```

henb-association [all | csg-id *csg_id_value*| full | henbgw-access-service *henbgw_acc_svc_name* | peer-address *peer_ip_address* | peer-id *peer_id_value* | summary | tai mcc *mcc_val* mnc *mnc_val* tac] | name *name*

henb-association : Displays information about HeNB associations.

all: Displays information about all HeNBGW Access services.

csg-id: Displays information about HeNB associations for the specified CSG ID.

csg_id_value is an integer between 0 and 4294967295.

full: Displays all available information for associated display or filter keyword (previous keyword).

henbgw-access-service: Displays information about HeNB associations with the specified HeNBGW Access service.

henbgw_acc_svc_name is an alphanumeric string of 1 through 63 characters.

peer-address: Displays information about HeNB associations with the specified peer.

peer_ip_address is an IPv4 address in dotted-decimal notation or an IPv6 address in colon-separated-hexadecimal notation.

peer-id: Displays information about HeNB associations for the specified peer.

peer_id_value is an integer from 0 to 4294967295.

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

tai: Displays information about HeNB associations for the specified TAI.

mcc: Specifies a Mobile Country Code (MCC) as a three-digit number between 100 to 999.

*mcc_val*is MCC value. MCC values of 000-099 are Reserved codes.

mnc: Specifies the Mobile National Code (MNC).

*mnc_val*is MCC a two- or three-digit number between 00 to 999.

tac: Displays information about HeNB associations for the specified Type Allocation Code (TAC).

miscellaneous : Displays all available information for associated display or filter keyword (previous keyword).

name*name* statistics [henbgw-access-service *henbgw_acc_svc_name* | miscellaneous [verbose] | peer-id *peer_id_value*s1ap [cause | [verbose]] | sctp [buffer [sessmgr *sessmgr_value*

name: Displays information for specific HeNBGW Access service name.

name: is an alphanumeric string of 1 through 63 characters.

statistics: Displays HeNBGW Access service statistics

miscellaneous : Displays Miscellaneous statistics.

s1ap: Displays S1AP statistics.

cause: Displays S1AP cause statistics.

sctp: Displays SCTP statistics.

buffer: Displays SCTP TX/RX buffer statistics.

sessmgr: Displays SCTP TX/RX buffer statistics on a specific sessmgr.

verbose: Specifies the verbosity.

| { 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 HeNBGW Access service related information.

Example

The following command displays S1AP statistics:

```
show henbgw-access-service statistics s1ap
```

show henbgw-network-service

Important

In Release 20, 21.0 and 21.1, HeNBGW is not supported. This command must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

This command displays configuration for HeNBGW Network service.

Product

HeNBGW

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show henbgw-network-service { all | mme-association [ all | full |
henbgw-network-service  henbgw_net_svc_name | peer-address peer_ip_address  |
peer-id peer_id_value | summary ]  | name name | statistics [
henbgw-network-service henbgw_net_svc_name | peer-id peer_id_value | s1ap [
cause | [ verbose ] ] | sctp [ buffer [ henbgwmgr  henbgwmgr_value]  ]  [
verbose ] ]  [ | { grep grep_options | more } ] }
```

henb-association [all | csg-id *csg_id_value*| full | henbgw-access-service *henbgw_acc_svc_name* | peer-address *peer_ip_address* | peer-id *peer_id_value* | summary] | name *name*

mme-association : Displays information about MME associations.

all: Displays all HeNBGW Network services.

full: Displays all available information for associated display or filter keyword (previous keyword).

henbgw-network-service: Displays information about HeNB associations with the specified HeNBGW Network service.

henbgw_net_svc_name is an alphanumeric string of 1 through 63 characters.

peer-address: Displays information about HeNB associations with the specified peer.

peer_ip_address is an IPv4 address in dotted-decimal notation or an IPv6 address in colon-separated-hexadecimal notation.

peer-id: Displays information about HeNB associations for the specified peer.

peer_id_value is an integer from 0 to 4294967295.

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

name*name*statistics [henbgw-network-service *henbgw_net_svc_name* | peer-id *peer_id_value*s1ap [cause | [verbose]] | sctp [buffer [henbgwmgr *sessmgr_value*

name: Displays information for specific HeNBGW Network service name.

name: is an alphanumeric string of 1 through 63 characters.

statistics: Displays statistics for specified object.

s1ap: Displays S1AP statistics.

cause: Displays S1AP cause statistics.

sctp: Displays SCTP statistics.

buffer Displays SCTP TX/RX buffer statistics.

henbgwmgr: Displays SCTP TX/RX buffer statistics on a specific henbgwmgr.

verbose: Specifies the verbosity.

| { 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 HeNBGW Network service related information.

Example

The following command displays S1AP Cause statistics :

```
show henbgw-network-service statistics s1ap cause
```

show hexdump-module

This command displays hexdump module related information.

Product

ePDG

SaMOG

Privilege

Administrator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]`*host_name*`#`

Syntax Description

```
show hexdump-module { file-space-usage | statistics } [ | { grep grep_options
 | more } ]
```

file-space-usage

Displays information about the file space usage of hexdump records.

statistics

Displays information on various statistics related to hexdump records.

| { 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 hexdump module related information.

Example

The following command displays information about the file space usage of hexdump records:

```
show hexdump-module file-space-usage
```

show hnbgw access-control-db

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 white list of IMSI records in the Access Control database residing on Home NodeB Gateway (HNB-GW) service instances that control HNB and UE access to HNB-GW sessions.

Product HNBGW

Privilege Inspector

Command Modes Exec

The following prompt is displayed in the Exec mode:

`[local]`*`host_name#`*

Syntax Description

```
show hnbgw access-control-db { hnbgw-servicehnbgw_svc_name | imsi imsi_value}
```

hnbgw-service *hnbgw_svc_name*

Displays Access Control database records for an existing HNB-GW service specified as an alphanumeric string of 1 through 63 characters.

Note This keyword is not supported in StarOS 14.0 and higher releases.

imsi *imsi_value*

Specifies the International Mobile Subscriber Identification (IMSI) number which is found on the Access Control database for he HNB-GW service.

imsi_value is an integer consisting of the 3-digit MCC (Mobile Country Code), the 2- or 3-digit MNC (Mobile Network Code) followed by the MSIN (Mobile Subscriber Identification Number). The total IMSI value must not exceed 15 digits.

Usage Guidelines This command displays the white list IMSI records in an Access Control database residing on a system support all Home-NodeB Gateway (HNB-GW) service instances. The white list controls HNB and UE access to HNB-GW sessions. Access Control database records can be filtered by IMSI value.

Example

The following command displays the information for registered IMSIs and their status in the HNB-GW database:

```
show hnbgw access-control-db imsi
```

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

show hnbgw 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 Home-NodeB Gateway (HNB-GW) services connected on this system.

Product

HNBGW

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show hnbgw counters [ hnbgw-service hnbgw_svc_name | hnbid hnb_identifier ] [
| { grep grep_options | more } ]
```

hnbgw-service *hnbgw_svc_name*

Filters the counter display based on an existing HNB-GW service name specified as an alphanumeric string of 1 through 63 characters.

hnbid *hnb_identifier*

Filters the counter display based on a Home-NodeB identifier specified as an alphanumeric string of 1 through 255 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 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-GW services configured and HNBs connected on this system.

Example

The following command displays the counters for the HNB-GW service named *hnbgw1*:

```
show hnbgw counter hnbgw-service hnbgw1
```

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

show hnbgw-global

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 global configuration parameters for configured HNBGW service(s) on this system.

Product HNBGW

Privilege Inspector

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show hnbgw-global
```

Usage Guidelines Use this command to view the global configuration parameters set for all HNBGW service(s) on this system.

Example

The following command displays the global configuration parameters applicable for all HNBGW services configured on this system:

```
show hnbgw-global
```

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

show hnbgw 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.

Displays the active/dormant session information about registered HNB(s) on Home-NodeB Gateway (HNB-GW) service instances configured and running on this system based on different filter criteria.

Product

HNBGW

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show hnbgw sessions [full | summary] [all] [address hnb_ip_address | cell-id
cell_id | hnb-access-mode {closed| hybrid | open } | hnb-local-id hnb_id |
hnbgw-service hnbgw_svc_name [ hnb-access-mode { closed | hybrid | open }]|
hnbid hnb_glbl_id | mcc mcc | mnc mnc [lac lac | rac rac | rnc rnc]] [ | {grep
grep_options | more }]
```

full

Displays the full information for a specific registered HNB session(s) on an HNB-GW service instance running on the system. The display can be filtered based on given filtering criteria.

summary

Displays summarized information for a specific registered HNB session(s) on an HNB-GW service instance running on the system. The display can be filtered based on given filtering criteria.

all

Displays summarized information for all registered HNB sessions on an HNB-GW service instance running on the system. The display can be filtered based on given filtering criteria.

address *hnb_ip_address*

Filters the display of full or summarized session statistics to show only HNB session(s) based on the registered HNB IP address expressed in IPv4 dotted-decimal notation.

cell-id *cell_id*

Filters the display of full or summarized session statistics to show only HNB session(s) based on the registered Femto cell ID where the user/subscriber is geographically located. and must be an integer from 0 through 268435455.*cell_id* is an integer from 0 through 268435455.

hnb-access-mode {closed | open | hybrid }

Filters the display of full or summarized session statistics to show only HNB session(s) based on the HNB access mode in an HNB-GW service instance.

- **closed** filters the session statistics for closed HNBs connected with HNB-GW service instance in Closed Access mode.
- **hybrid** filters the session statistics for hybrid HNBs connected with HNB-GW service instance in Hybrid Access mode.

- **open** filters the session statistics for open HNBs connected with HNB-GW service instance in Open Access mode.

hnb-local-id *hnb_id*

Filters the display of full or summarized session statistics to show only HNB session(s) based on the registered local ID of HNB specified as an integer from 1 through 25.

hnbgw-service *hnbgw_svc_name*

Filters the display of session statistics to show only registered HNB session(s) based on an existing HNB-GW service name specified as an alphanumeric string of 1 through 63 characters.

This can be further filtered by using access-mode criteria: Closed, Hybrid, or Open.

hnbid *hnb_glbl_id*

Displays summarized or full information of HNB session(s) based on the registered global ID of HNB specified as an integer between 1 through 255.

mcc *mcc*

Displays summary information of HNB session(s) based on the registered Mobile Country Code (MCC) identification number of the UE specified as an integer between 101 through 999.

mnc *mnc*

Displays summarized or full information of HNB session(s) based on the registered Mobile Network Code (MCC) identification number of the UE specified as a 2- or 3-digit integer between 00 through 999.

lac *lac*

Displays summarized or full information for HNB session(s) based on the registered Location Area Code (LAC) identification number of the UE specified as an integer between 1 through 65535.

rac *rac*

Displays summarized or full information for HNB session(s) based on the registered Radio Access Code (RAC) identification number of the UE specified as an integer between 1 through 255.

rnc *rnc*

Displays summarized or full information for HNB session(s) based on the registered Radio Network Code (RAC) identification number of the HNB specified as an integer between 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 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 statistics of all or specific registered HNB session(s) or in selected part of user session for HNB-GW services configured and running on this system.

Example

The following command displays summarized session statistics for all registered HNBs on the HNB-GW service named *hnbgw1*:

```
show hnbgw sessions summary hnbgw-service hnbgw1
```

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

show hnbgw statistics hnbgw-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 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 hnbgw statistics [ gtpu-only ] [ hnb-access-mode { closed | hybrid | open }] [ hnbgw-service hnbgw_svc_name [ gtpu-only | hnb-access-mode { closed | hybrid | open } | hnbap-only | ipne-only | paging-only | ranap-only | rtp-only | rua-only | sabp-only | sctp-only ] ] [ hnbid hnb_identifier ] [ hnbap-only | ipne-only | paging-only |ranap-only | rua-only | sccp-only | sctp-only ] ] [ verbose] [ | { grep grep_options | more } ]
```

gtpu-only

Displays Forwarded GTPU Pkt statistics for selected HNB/HNBGW Service.

hnb-access-mode { closed | hybrid | open }

Displays the session statistics of an existing HNB-GW service based on access mode filters. Other supported filters are:

- **closed**: shows the statistics of only those UEs which are connected through Closed HNBs to the HNB-GW services on a chassis. This command applies to all Closed HNB sessions on a chassis. If any other criteria specified it will filter the statistics based on given criteria.

- **hybrid**: shows the statistics of only those UEs which are connected through Hybrid HNBs to the HNB-GW services on a chassis. This command applies to all Closed HNB sessions on a chassis. If any other criteria specified it will filter the statistics based on given criteria.
- **open**: shows the statistics of only those UEs which are connected through Open HNBs to the HNB-GW services on a chassis. This command applies to all Closed HNB sessions on a chassis. If any other criteria specified it will filter the statistics based on given criteria.

hnbgw-service *hnbgw_svc_name*

Filters the display of session statistics for an existing HNB-GW service name specified as an alphanumeric string of 1 through 63 characters.

hnbap-only

Filters the display of session statistics to show only Home NodeB Application Part (HNBAP) traffic for the selected HNB-GW service which is configured and running on this system.

ipne-only

Filters the display of session statistics to show only IPNE for selected HNBGW Service which is configured and running on this system.

paging-only

Filters the display of Paging statistics for selected HNBGW Service.

ranap-only

Flitters the display of session statistics t to show only Radio Access Network Application Protocol (RANAP) traffic for the selected HNB-GW service which is configured and running on this system.

rua-only

Filters the display of session statistics to show only RANAP User Adaptation (RUA) traffic for the selected HNB-GW service which is configured and running on this system.

sccp-only

Filters the display of session statistics to show only Signaling Connection Control Part (SCCP) traffic for the selected HNB-GW service which is configured and running on this system.

sctp-only

Filters the display of session statistics to show only Stream Control Transmission Protocol (SCTP) traffic for selected HNB-GW service which is configured and running on this system.

verbose

Displays detailed statistics for all sessions on HNB-GW services or for a selected filtered and named HNB-GW service which is configured and 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.

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 session statistics for the HNBAP part of session details for the HNB-GW service named *hnbgw1*:

```
show hnbgw statistics hnbgw-service hnbgw1 hnbap-only
```

The following command displays session statistics for the RANAP part of session with maximum details for the HNB-GW service named *hnbgw1*:

```
show hnbgw statistics hnbgw-service hnbgw1 ranap-only verbose
```

show hnbgw statistics hnbid

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 for Home-NodeB (HNB) connected to an HNB-GW service on this system.

Product

HNBGW

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show hnbgw statistics hnbid hnb_identifier [ hnbap-only | ranap-only | rua
-only] [ verbose] [ | { grep grep_options | more } ]
```

hnbid *hnb_identifier*

Filters the display of session statistics based on an existing Home-NodeB identifier specified as an alphanumeric string of 1 through 255 characters.

hnbap-only

Filters the display of session statistics display to show only Home NodeB Application Part (HNBAP) traffic for the selected HNB which is connected to this system through HNB-GW service.

ranap-only

Filters the display of session statistics display to show only Radio Access Network Application Protocol (RANAP) traffic for the selected HNB which is connected to this system through HNB-GW service.

rua-only

Filters the display of session statistics display to show only RANAP User Adaptation (RUA) traffic for the selected HNB which is connected to this system through HNB-GW service.

verbose

Displays detailed statistics for all HNB sessions or for the selected filter and HNB which is connected to this system through HNB-GW service.

| { 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 the *Command Line Interface Overview* chapter.

Usage Guidelines

Use this command to view the session statistics for overall session or in selected part of user session for selected HNB which is connected to this system through HNB-GW service.

Example

The following command displays session statistics for the HNBAP part of session details for the HNB identified as *hnb112234* on this system:

```
show hnbgw statistics hnbid hnb112234 hnbap-only
```

The following command displays detailed session statistics for the RANAP part of session details for the HNB identified as *hnb112234* on this system:

```
show hnbgw statistics hnbid hnb112234 ranap-only verbose
```

show hnbgw-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 configuration details for configured HNBGW service(s) on this system.

Product

HNBGW

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show hnbgw-service { all | hnbgw-service hnbgw_svc_name }
```

all

Displays configuration and other default parameters for all HNB-GW service configured on this system.

hnbgw-service *hnbgw_svc_name*

Displays configuration and default parameters for an existing HNB-GW service name specified as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to view the configuration and service parameters set for all or any specific HNB-GW service(s) on this system.

Example

The following command displays configuration parameters for all HNB-GW services configured on this system:

```
show hnbgw-service all
```

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

show hsgw-service

Displays information for HRPD Serving Gateway (HSGW) services on this system.

Product

HSGW

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show hsgw-service { all | name service_name | statistics { all | name service
_name } } [ dns-stats | pcf-status [ address IPv4_address | filter { all |
icmp-monitored | no-calls | summary | up } ] ] [ | { grep grep_options |
more } ]
```

all

Displays configuration information for all HSGW services configured on this system.

name *service_name*

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

statistics

Displays node-level statistics for the HSGW.

dns-stats

Displays information related to DNS P-GW selection for load balancing using DNS SRV lookup.

pcf-status

Displays information about the status of Packet Control Functions (PCFs) being monitored.

address *IPv4_address*

Displays status information for the specified PCF.

IPv4_address must be specified using IPv4 dotted-decimal notation.

filter { all | icmp-monitored | no-calls | summary | up }

Filters the PCF status information. Must be followed by the filter to be applied.

all: Shows all the PCFs.

icmp-monitored: Shows only PCFs which are ICMP monitored.

no-calls: Shows only PCFs which has no active sessions.

summary: Shows only a summary of the status of the PCFs.

up: Shows only PCFs which are alive.

| { 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 the *Command Line Interface Overview* chapter.

Usage Guidelines

Use this command to view configuration information for HSGW services on this system.

Example

The following command displays service statistics for the HSGW service named *hsgw1*:

```
show hsgw-service name hsgw1
```

show hss-peer-service

Displays service, session, and statistics information for Home Subscriber Server (HSS) peer services configured on this system.

Product

MME

Privilege

Inspector

Syntax Description

```
show hss-peer-service { service { all | name name } | session { all |
callid id | full | mdn mdn | nai nai | summary } | statistics { all | service
 name | summary } } [ | { grep grep_options | more } ]
```

service { all | name *name* }

Displays HSS peer service statistics for HSS peer services configured on this system.

all: Displays HSS peer service statistics for all configured HSS peer services on this system.

name *name*: Displays HSS peer service statistics for an existing HSS peer service specified as an alphanumeric string of 1 through 63 characters.

session { all | callid *id* | full | mdn *mdn* | nai *nai* | summary }

Displays HSS peer service statistics for sessions on this system.

all: Displays HSS peer service statistics for all sessions on this system.

This keyword is also used to further filter the **full** and **summary** options.

callid *id*: Displays summarized or detailed statistics of HSS peer service sessions running and filtered on the basis of the call identifier specified as an 8-digit hexadecimal number.

This keyword is also used to further filter the **full** and **summary** options.

mdn *mdn*: Displays summarized or detailed statistics of MME sessions running and filtered on the basis of an existing Mobile Directory Number (MDN) expressed as an alphanumeric string of 1 through 100 characters.

This keyword is also used to further filter the **full** and **summary** options.

nai *nai*: Displays summarized or detailed statistics of MME-HSS sessions running and filtered on the basis of an existing Network Access Identifier (NAI) expressed as an alphanumeric string of 1 through 128 characters.

This keyword is also used to further filter the **full** and **summary** options.

summary: Displays a summarized output of session information. This keyword can be further filtered by adding the following options:

- **full**

- **callid** *id*
- **mdn** *mdn*
- **nai** *nai*

statistics { all | service *name* | summary }

Displays statistics for HSS peer services configured on this system.

all: Displays statistics for all HSS peer services configured on this system.

service *name*: Displays statistics for a an existing HSS peer service expressed as an alphanumeric string of 1 through 63 characters.

summary: Displays summarized statistics for all HSS peer services configured 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 *CLI Overview* chapter of the *Command Line Interface Reference*.

Usage Guidelines

Use this command to display service, session, and statistics information for HSS peer services configured on this system.

Example

The following command displays HSS peer service information and statistics for a session with a call ID of *08f11fa4*:

```
show hss-peer-service sessions full callid 08f11fa4
```

show imei-profile

Displays information for configured International Mobile Equipment Identity (IMEI) profiles.

Product

SGSN

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show imei-profile { all | full { all | name imei_name } | name imei_name } [
 | { grep grep_options | more } ]
```

all

Lists all IMEI profiles configured on the system.

full { all | name *apn_name* }

full: Instructs the system to display all information in the IMEI profile(s).

all: Displays a full set of information for all IMEI profiles configured on the system.

name *imei_name*: Displays a full set of information for a specific IMEI profile.

apn_name: Must be an existing IMEI profile expressed as an alphanumeric string of 1 through 64 characters.

name *imei_name*

Displays information for a specific IMEI profile expressed 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 IMEI profiles configured on the system. APN profiles are configured through the global configuration mode and in the IMEI profile configuration mode. For more information regarding IMEI profile commands, refer to the *IMEI Profile Configuration Mode Commands* chapter.

Example

The following command displays all available information for an IMEI profile named *imeiprof1*:

```
show imei-profile full name imeiprof1
```

show ims-authorization policy-control

Displays information and statistics specific to the policy control in IP Multimedia Subsystem (IMS) authorization service.

Product

SCM

GGSN

IMS

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 ims-authorization policy-control statistics [ service ims_auth_svc_name
 | server { ip-address ip_address [ port port_value ] | name server_name } ] [
 | { grep grep_options | more } ]
```

statistics

Displays the total collected statistics of all policy control parameters of IMS authorization service sessions since the last system **restart** or **clear** command.

service *ims_auth_svc_name*

Displays the total collected statistics of all IMS authorization sessions processed by a specific IMS authorization service since the last system restart or clear command. *ims_auth_svc_name* must be an existing IMS authorization service name, expressed as an alphanumeric string of 1 through 64 characters.

server { ip-address *ip_address* [port *port_value*] | name *server_name* }

Displays the server-level message statistics and the server IP address.

Specify the PCRF server name (1 through 64 alphanumeric characters), or server IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal 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 **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 and statistics about policy control configuration in existing IMS authorization services.

Example

The following command displays the existing IMS authorization service name *ims_auth_gx1* on the system:

```
show ims-authorization policy-control statistics service ims_auth_gx1
```

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

show ims-authorization policy-control misc-info

Displays the maximum backpressure information.

Product

GGSN

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 ims-authorization policy-control misc-info max-backpressure [ all |
 facility sessmgr instance instance_number ] [ | { grep grep_options | more }
]
```

all

Displays the max-backpressure count among all active 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.

instance_number must be an existing IMS authorization service name, expressed as an alphanumeric string of 0 to 10000000 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 the maximum backpressure at a particular session manager instance or at all instances, and the time stamp at which maximum backpressure was seen.

Example

The following command displays the maximum backpressure information for *session1* facility on the system:

```
show ims-authorization policy-control misc-info max-backpressure facility
 sessmgr instance  session1
```

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

show ims-authorization policy-gate

Displays information of installed Policy Gates for specific subscriber in an IP Multimedia Subsystem (IMS) authorization (IMSA) service.

Product

SCM

GGSN

IMS

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 ims-authorization policy-gate { { status [ summary | full ] [ { imsi
 imsi_value [ nsapi nsapi_value ] } | callid call_id | { ims-auth-service
ims_auth_svc } [ rulename rule_name ] } | { counters [ all | { imsi imsi_value
[ nsapi nsapi_value ] } | { rulename rule_name} | { callid call_id } ] } [ | {
 grep grep_options | more } ] ]
```

status [summary | full]

Displays the status of the installed policy gates and their flow definitions along with the run-time status in an IMS authorization service based on the specified criteria.

summary: Limits the display to a summary on the status of the installed policy gates and their flow definitions along with their run-time status in an IMS authorization service based on the specified criteria.

full: Displays the full information on status of the installed policy gates and their flow definitions along with their run-time status in an IMS authorization service based on the specified criteria.

counters all

Displays the counters/statistics of the installed policy gates and their flow definitions along with their run-time status in an IMS authorization service based on the specified criteria.

all displays all counters of the installed gates and their flow definitions along with their run-time status in an IMS authorization service based on the specified criteria.

imsi *imsi_value* [nsapi *nsapi_value*]

Displays all of the counters/status of the installed policy gates and their flow definitions along with the run-time status in an IMS authorization service based on the International Mobile Subscriber Identity (IMSI).

nsapi *nsapi_value* specifies the Network Service Access Point Identifier (NSAPI) and limits the display to a single PDP context of the subscriber.

callid *call_id*

Displays all of the counters/status of the installed policy gates and their flow definitions along with their run-time status in an IMS authorization service based on the call identifier.

ims-auth-service *ims_auth_svc*

Displays the status of the installed policy gates and their flow definitions along with their run-time status in the named IMS authorization service.

rulename *rule_name*

Displays all of the counters/status of the installed policy gates and their flow definitions along with their run-time status in an IMS authorization service based on the named dynamic charging rule.

| { 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.

Please refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference* for details on the usage of **grep** and **more**.

Usage Guidelines

Use this command to display information/statistics/counters about all of the installed policy gates and their flow definitions along with the run-time status with specified criteria and filters in existing IMS authorization services.

Example

The following command displays the full status of the installed policy gates in an existing IMS authorization service on the system:

```
show ims-authorization policy-gate status full
```

The following command displays the all counters of the installed policy gates in an existing IMS authorization service on the system:

```
show ims-authorization policy-gate counters all
```

Important

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

show ims-authorization servers

Displays information and statistics specific to the authorization servers used for IP Multimedia Subsystem (IMS) authorization (IMSA) service.

Product

SCM

GGSN

IMS

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]`*`host_name`*`#`

Syntax Description

```
show ims-authorization servers [ ims-auth-service ims_auth_svc_name [ | {
grep grep_options | more } ] ]
```

server [ims-auth-service *ims_auth_svc_name*]

Displays the information and statistics for all authorization servers configured within an IMS authorization service in a system.

ims-auth-service *ims_auth_svc_name*: Displays the configured authorization servers for IMS authorization within the named IMS authorization service.

| { 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.

Please refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference* for details on the usage of **grep** and **more**.

Usage Guidelines

Use this command to display information and statistics about IMS authorization servers configured on a system or IMS authorization service.

Example

The following command displays the information and statistics of the authorization servers in the IMS authorization service named in *ims_auth_gx1*:

```
show ims-authorization servers ims-auth-service ims_auth_gx1
```

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

show ims-authorization service

Displays information, configuration, and statistics of all/specific IP Multimedia Subsystem (IMS) authorization (IMSA) service.

Product

GGSN

P-GW

SAEGW

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show ims-authorization service { { all [ verbose ] | name ims_auth_svc_name [ p-cscf { all | ip_address ipv4/ipv6_address | summary ] } | { statistics [ all | name ims_auth_svc_name ] [ verbose ] } [ | { grep grep_options | more } ]
```

all [verbose]

Displays information and configuration for all configured IMS authorization services with a single line of information for each IMS authorization service.

verbose: Displays all information and configuration data for all IMS authorization services configured on system.

name *ims_auth_svc_name* [p-cscf { all | ip_address *ipv4/ipv6_address*

Displays the information, statistics, and configuration data for the named IMS authorization service. If the optional keyword is configured, this command displays the statistics information of all P-CSCF servers or specific server.

summary

Displays summarized information and configuration data for all IMS authorization services configured in a system.

statistics [all | name *ims_auth_svc_name*] [verbose]

Displays the IMS Authorization service statistics including following information:

- Initial authorization procedures
- Re-authorization procedures initiated by us
- Re-authorization procedures initiated by servers
- Various failure statistics

If no criteria are specified, only summarized statistics for all IMS Authorization services are displayed

- **all**: displays individual statistics for every IMS authorization service configured on system.
- name *ims_auth_svc_name*: Displays the statistics for the IMS authorization service named in *ims_auth_svc_name*
- verbose: displays detailed statistics for a configured IMS authorization service.

| { 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.

Please refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference* for details on the usage of **grep** and **more**.

Usage Guidelines

Use this command to display the status, counters and configuration. for an IMS Authorization service. The status includes the state of a server table switchover. The Statistics option displays information about various processes.

Example

The following command displays the information and configuration data of the IMS authorization service named in *ims_auth_gx1*:

```
show ims-authorization service name ims_auth_gx1
```

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

show ims-authorization sessions

Displays information, configuration, and statistics of sessions active in an IP Multimedia Subsystem (IMS) authorization (IMSA) service.

Product

SCM

GGSN

IMS

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show ims-authorization sessions [ all | apn apn_name | callid call_id |
facility sessmgr instance instance_no | full | ggsn-only | ims-auth-service
 ims_auth_svc_name | imsi  imsi_value [ nsapi  nsapi_value ]| ip-address  ip_address
 | local-sessions | remote-sessions | summary ] [ | { grep grep_options |
more } ] ]
```

all

Displays information and configuration for all sessions running in IMS authorization services with a single line of information for each IMS authorization session.

apn *apn_name*

Displays all of the counters/status for the running services in an IMS authorization service based on the specified Access Point Name (APN).

callid *call_id*

Displays all of the counters/status for the running services in IMS authorization service based on the named call identifier.

facility sessmgr instance *instance_no*

Displays the IMS authorization sessions at the session manager instance level.

full

Displays complete information and configuration data for all sessions in IMS authorization services configured in a system.

ggsn-only

Displays GGSN-specific information in addition to detailed information about the session.

ims-auth-service *ims_auth_svc_name*

Displays the information, statistics, and configuration data for sessions in the named IMS authorization service.

imsi *imsi_value* [nsapi *nsapi_value*]

Displays all of the counters/status of the running services in an IMS authorization service based on the specified International Mobile Subscriber Identity (IMSI) and Network Service Access Point Identifier (NSAPI). The display is limited to a single PDP context of the subscriber.

ip-address *ip_address*

Displays all of the counters/status for the running services in IMS authorization service based on the specified host IP address.

local-sessions

Displays the IMS authorization sessions that are associated with local-policy.

remote-sessions

Displays the IMS authorization sessions that are associated with PCRF.

summary

Displays summarized information and configuration data for all IMS authorization services configured in a 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.

Please refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference* for details on the usage of **grep** and **more**.

Usage Guidelines

Use this command to display the sessions running under IMS Authorization service on a system with different filter criteria.

Example

The following command displays the information and statistical data for a session in an IMS authorization service:

```
show ims-authorization sessions full
```

Important

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

show instance-logging

Displays the instance numbers for all currently enabled, facility-specific log instances.

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 instance-logging facility facility_name[ | { grep grep_options | more } ]
```

facility *facility_name*

Specifies the facility for which instance-level logging has been enabled. *facility_name* can be aaamgr, hamgr or sessmgr.

| { 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 the *Command Line Interface Overview* chapter.

Usage Guidelines

Displays the instance numbers for all currently enabled, facility-specific log instances. These instances have been previously enabled via the Exec mode **logging filter enable facility** command.

Example

The following command displays instance-specific logging enabled for the sessmgr facility:

```
show instance-logging facility sessmgr
```

show inventory

Displays Unique Device Identifier (UDI) information for all hardware in the system for which a UDI is available.

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

Usage Guidelines

Displays UDI information (card/item description, Cisco PID, serial number) for all hardware installed in this system.

Example

The following command displays UDI information for all cards in the system:

```
show inventory
```

show ip access-group statistics

Displays statistics for each rule in an access control group.

Product

HA

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show ip access-group statistics [ | { 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 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 configured access control groups in the current context.

Example

The following command displays the contents of an access control group named *ACG_4*:

```
show ip access-list ACG_4
```

show ip access-list

Displays the information for all Access Control Lists (ACLs) or the named ACL. With no keyword supplied, a list of all access lists and their entries is displayed.

Product

HA

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show ip access-list list_name [ | { grep grep_options | more } ]
```

list_name

Specifies the name of an existing ACL configured in the current context as an alphanumeric string of 1 through 47 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 the configured ACLs in the current context.

Example

The following command displays the contents of an ACL named *ACL_4*:

```
show ip access-list ACL_4
```

show ip arp

Displays the ARP table or the ARP information associated with the specified IP address.

Important When it restarts, the VPN Manager removes all interfaces from the kernel; the kernel then removes all ARP entries. When this happens, the NPU still holds all of the ARP entries so that there is no traffic disruption. From a user point of view, **show ip arp** is broken since this command gathers information from the kernel and not the NPU.

Product

HA

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show ip arp [ ip_address | vrf vrf_name ] [ | { grep grep_options | more } ]
```

ip_address

Specifies an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

| vrf *vrf_name*

Displays information for an existing VPN Routing and Forwarding (VRF) name expressed 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 display the configured ACLs in the current context.

Example

The following command displays the contents of an ACL named *ACL_4*:

```
show ip access-list ACL_4
```

show ip as-path-access-list

Displays the contents of a Border Gateway Protocol (BGP) router Autonomous System (AS) path access list in the current context.

Product

HA

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]`*`host_name`*`#`

Syntax Description

```
show ip as-path-access-list list_name [ | { grep grep_options | more } ]
```

list_name

Specifies the name of an existing AS path access list configured in the current context 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

Use this command to display the configured entries for the specified BGP router AS path access list in the current context.

Example

The following command displays the contents of an AS path access list named *ASlist1*:

```
show ip as-path-access-list ASlist1
```

show ip bgp

Displays Border Gateway Protocol (BGP) information for the current context.

Product

HA

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show ip bgp [ ip_address/mask | debugging | filter-list list_name  | neighbors
 [ ip_address ] | route-map map_name | vpnv4 [ all [ ip_address/mask | neighbors
 | summary ] | route-distinguisher { ipv4_address | asn_value } rd_value | vrf
vrf_name [ ip_address/mask | neighbors | summary ] | vpnv6 [ all [ ipv4_ddress |
 neighbors | summary ] | route-distinguisher { ipv4_address | asn_value } rd_value
 | vrf vrf-name [ ip_address/mask | neighbors | summary ] ] [ | { grep grep_options
 | more } ]
```

ip_address/mask

Specifies the IP address and netmask bits for the network for which information should be displayed. The IP address and mask is the number of subnet bits, representing a subnet mask in CIDR notation. These must be entered in the IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal CIDR notation.

debugging

Displays debug flags that are enabled.

filter-list *list_name*

Displays routes that match the specified filter list.

neighbors [*ip_address*]

Displays information for all neighbors or a neighbor specified as an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

route-map *map_name*

Displays routes that match the specified route-map.

summary

Displays summary BGP information.

| vpnv4 [all [*ip_address/mask* | neighbors | summary] | route-distinguisher { *ipv4_address* | *asn_value* } *rd_value* | vrf *vrf_name* [*ip_address/mask* | neighbors | summary]

Displays all VPNv4 routing data.

- **all**: Displays all VPNv4 routing information. If this is specified, the information displayed is gathered from all the VRF's known to BGP and displayed. It could contain the list of neighbors, the list of networks, or a particular network.
- **neighbors**: Displays neighbor information for the all the VRFs including the default VRF or for the VRF with a matching RD value.
- **summary**: Displays summary information of neighbors for all the VRFs including the default VRF or for the VRF with a matching RD value.

- **route-distinguisher {** *ipv4_address* | *asn_value* **}** *rd_value*: Displays information about the route distinguisher. Where
  - *ipv4_address*: Specifies an IP address in IPv4 dotted-decimal notation.
  - *asn_value*: Specifies an autonomous system number as an integer from 0 through 65535.
  - *rd_value*: Specifies a route distinguisher value as an integer from 0 through 4294967295.
- **vrf** *vrf_name* **[** *ipv4_address/mask* **|** **neighbors** **|** **summary** **]**: Displays information about the VRF. Where
  - *vrf_name*: Specifies the name of the VRF as an alphanumeric string of 1 through 63 characters.
  - *ip_address/mask*: Specifies an IP address in IPv4 dotted-decimal CIDR notation.
  - **neighbors**: Displays neighbor information for the all the VRFs including the default VRF or for the VRF with a matching RD value.
  - **summary**: Displays summary information of neighbors for all the VRFs including the default VRF or for the VRF with a matching RD value.

| vpnv6 [all [*ipv4_ddress* | neighbors | summary] | route-distinguisher { *ipv4_address* | *asn_value* } *rd_value* | vrf *vrf-name* [*ip_address/mask* | neighbors | summary]]

Displays all VPNv6 routing data.

- **all**: Displays all VPNv6 routing information. If this is specified, the information displayed is gathered from all the VRF's known to BGP and displayed. It could contain the list of neighbors, the list of networks, or a particular network.
- **neighbors**: Displays neighbor information for the all the VRFs including the default VRF or for the VRF with a matching RD value.
- **summary**: Displays summary information of neighbors for all the VRFs including the default VRF or for the VRF with a matching RD value.
- **route-distinguisher {** *ipv4_address* | *asn_value* **}** *rd_value*: Displays information about the route distinguisher. Where
  - *ipv4_address*: Specifies an IP address in IPv4 dotted-decimal notation.
  - *asn_value*: Specifies an autonomous system number as an integer from 0 through 65535.
  - *rd_value*: Specifies a route distinguisher value as an integer from 0 through 4294967295.
- **vrf** *vrf_name* **[** *ipv4_address/mask* **|** **neighbors** **|** **summary** **]**: Displays information about the VRF. Where
  - *vrf_name*: Specifies the name of the VRF as an alphanumeric string of 1 through 63 characters.
  - *ip_address/mask*: Specifies an IP address in IPv4 dotted-decimal CIDR notation.
  - **neighbors**: Displays neighbor information for the all the VRFs including the default VRF or for the VRF with a matching RD value.
  - **summary**: Displays summary information of neighbors for all the VRFs including the default VRF or for the VRF with a matching RD value.

| { 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 display to BGP information for the current context.

Example

The following command displays information for all BGP neighbors:

```
show ip bgp neighbors
```

show ip framed-prefixes

Displays the framed-prefixes along with session-id, vrf-name and pool-name. The command will also display the total number of framed-prefixes matching the filtering criteria.

Product

All

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

```
show ip framed-prefixes [ sess-id session_identifier | vrf vrf_identifier ]
```

sess-id *session identifier*

Displays framed-prefixes added by a specific session.

session_identifier must be an integer from 1 to 1152.

vrf *vrf_identifier*

Displays VRF specific routing information.

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

Usage Guidelines

Use this command to display the framed-prefixes. This command also enables filtering of framed-prefixes based on vrf-name and/or session-id to the display. The display will show framed-prefixes along with session-id, vrf-name, and pool-name. The command will also display the total number of framed-prefixes matching the filtering criteria.

Example

The following command displays ip framed-prefixes by a specific session.

```
show ip framed-prefixes sess-id session_identifer
```

show ip igmp group

Displays Internet Group Management Protocol (IGMP) information for all groups in a context or a specific IP address.

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 ip igmp group [ ip_address | all } [ | { grep grep_options | more } ]
```

ip_address

Displays IGMP information for the IP address specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

all

Displays information for all IGMP groups associated with this context.

| { 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 IGMP group information.

Example

To display general IGMP information for all groups in this context, enter the following command;

```
show ip igmp all
```

show ip interface

Displays statistical and configuration information for the IPv4-based interfaces, including a Virtual Routing and Forwarding (VRF) table for a specific 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 ip interface [ vrf vrf-name ] [ name intfc_name [ tunnel [ gre-keepalive
 ] ] [ summary ] [ vrf vrf-name ] [ | { grep grep_options | more } ]
```

name *intfc_name*

Displays information for an existing interface specified as an alphanumeric string of 1 through 79 characters. If no interface name is specified, the information for all IP interfaces is displayed.

summary

Displays summarized information about requested IP interfaces.

tunnel [gre-keepalive]

Filters the IP interface information for GRE/IP-in-IP tunnel type interfaces.

gre-keepalive: Displays the keepalive information for a generic routing encapsulation (GRE) tunnel configured with this IP interface.

vrf *vrf_name*

Displays Virtual Routing and Forwarding (VRF) routing information for an existing VRF 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 display the summarized of detailed configuration and statistical information for a configured IP interface. This information can be used to verify and/or troubleshoot communication difficulties between to a remote host/node.

Example

The following command displays the interface information, including statistics, for the IP interface *Interface_1*.

```
show ip interface Interface_1 statistics
```

The following command displays the GRE keepalive information for an IP interface named in *IP_gre1*.

```
show ip interface IP_gre1 tunnel gre-keepalive
```

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

show ip ipsp

Displays the names of IP pools that are enabled for the IP pool sharing protocol (IPSP) and lists the disposition of addresses in the pools.

Product

PDSN

HA

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 ip ipsp [ summary ] [ | { grep grep_options | more } ]
```

summary

Displays only the disposition of the addresses in the participating IP pools. Does not show the names of the participating IP pools.

| { 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 list the names of IP pools that are participating in the IPSP and list the disposition of IP addresses in those pools.

Important For information on configuring and using IPSP refer to the *System Administration Guide*.

Example

To list information on all IPSP participating pools and address disposition, enter the following command:

```
show ip ipsp
```

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

show ip localhosts

Displays host name to IP address mapping for current context. Must be followed by a specific IP host name.

Product

PDSN

HA

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 ip localhosts hostname [ | { grep grep_options | more ]
```

hostname

Specifies a configured hostname 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 display mappings of a host name to IP addresses.

Example

To display IP address mapping for host name *local_2345*, enter the following command;

```
show ip localhosts local_2345
```

show ip ospf

Displays Open Shortest Path First (OSPF) routing information.

Product

PDSN

HA

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 ip ospf [ border-routers | database [ verbose ] [ ls-id ip_addr ] [
adv-router ip_addr ] [ ls-type { router | network | summary | asbr-summary
 | external | nssa | integer } ] | debugging | interface | neighbor [ details
 ] | route | virtual-links  ] [ | { grep grep_options | more } ]
```

border-routers

Displays all known area border routers (ABRs) and autonomous system border routers (ASBRs) for OSPF.

database [verbose] [ls-id *ip_addr*] [adv-router *ip_addr*] [ls-type { router | network | summary | asbr-summary | external | nssa | *integer* }]

Displays a summary of the database information for OSPF.

verbose: Displays detailed OSPF database information.

ls-id *ip_addr*: Displays OSPF database information for the link state advertisements (LSAs) with the specified link state identifier (LSID). *ip_addr* is entered using IPv4 dotted-decimal notation.

adv-router *ip_addr*: Displays OSPF database information for the advertising router with the specified LSID. *ip_addr* is entered using IPv4 dotted-decimal notation.

ls-type { router | network | summary | asbr-summary | external | nssa | *LSA_Numerical_Type* **}]**: Displays OSPF database information for the specified LSA type.

debugging

Lists which debugging parameters are enabled.

interface

Displays interface information for OSPF.

neighbor [details]

Displays summarized information about all known OSPF neighbors.

details: Displays detailed information about all known OSPF neighbors.

route [summary]

Displays the OSPF routing table.

summary: Displays the number of intra-area, inter-area, external-1 and external-2 routes.

virtual-links

Displays the OSPF virtual links.

| { 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 OSPF information.

Example

To display general OSPF information, enter the following command;

```
show ip ospf
```

show ip policy-forward

Displays information for IP packet redirecting policy for Home Agent (HA).

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 ip policy-forward [ | { 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 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 see all the settings for IP packet redirection configuration from existing HA to new HA during upgrade.

Important This is a customer specific command.

Example

The following command displays forward policy configuration for an HA:

```
show ip policy-forward
```

show ip pool

Displays statistics specific to IP pools.

Product

PDSN

GGSN

HA

ASN-GW

A-BG

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show ip pool [ address { pool-name pool_name | group-name group_name } { used
 | free | hold | release } [ limit limit ] | group-name group_name | groups
 | hold-timer { imsi imsi | msid msid | username username [ imsi imsi | msid
msid ] } | many-to-one | nat-realm | one-to-one | overlap | pool-name
pool_name | private | public | resource | static | summary | verbose | wide
 ] [ | { grep grep_options | more }
```

address { pool-name *pool_name* | group-name *group_name* }{ used | free | hold | release} [limit *limit*]

Displays IP pool addresses for the specified IP pool or pool group that are currently in the specified state.

pool-name *pool_name*: Displays IP addresses from an existing IP pool name specified as an alphanumeric string of 1 through 31 characters.

group-name *group_name*: Displays IP addresses from an existing IP pool group name specified as an alphanumeric string of 1 through 31 characters.

used: Displays the IP addresses that are in a used state.

free: Displays the IP addresses that are in a free state.

hold: Displays the IP addresses that are in a hold state.

release: Displays the IP addresses that are in a release state.

limit *limit*: Specifies the maximum number of address to display as an integer from 1 through 524287.

group-name *group_name*

Displays information about an existing IP pool group name specified as an alphanumeric string of 1 through 31 characters.

groups

Lists information about all IP pool groups.

hold-timer {imsi *imsi* | msid *msid* | username *username* [imsi *imsi* | msid *msid*]}

Displays hold timer address information for the specified IMSI, MSID, or username.

imsi *imsi*: Displays hold-timer information for a valid IMSI (International Mobile Subscriber Identity), specified as a 15-character field that identifies the subscriber's home country and carrier.

msid *msid*: Displays hold-timer information for the MSID specified as a number from 7 through 16 digits.

username *username*: Displays hold-timer information for an existing username specified as an alphanumeric string of 1 through 127 characters.

Important Active users cannot be displayed. If an active ID or username is entered, the following error message appears: Failure: No address matching the specified information was found! Please confirm that the options used match the network architecture/deployment, such as IMSI/MSID only, Username only, or IMSI/MSID plus Username. Please note that this command does not apply for addresses in the used state.

many-to-one

Lists information on Many-to-One NAT Realm IP address pools.

nat-realm

Lists information on NAT Realm IP address pools.

one-to-one

Lists information One-to-One NAT Realm IP address pools.

overlap

Lists information on overlapping IP pools.

pool-name *pool_name*

Displays information about an existing IP pool.

private

Displays information about IP pools marked Private.

public

Displays information about IP pools marked Public.

resource

Displays information about resource IP pools.

static

Displays information about static IP pools.

summary

Displays a summary of all IP pool information.

verbose

Displays detailed information about all IP pools.

wide

Displays detailed information formatted to more than 80 columns.

| { 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 statistics pertaining to IP Pools in the current context.

Example

The following command displays IP address information for an IP Pool named *pool1*:

```
show ip pool address pool-name pool
```

To display a summary list for all IP pools in the current context, enter the following command:

```
show ip pool summary
```

The following command displays IP pool information for all IP pools configured in the current context:

```
show ip pool verbose
```

Important

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

show ip prefix-list

Displays IP prefix lists used to filter routes. With no keyword supplied, a list of all prefix lists and their entries is displayed.

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 ip prefix-list [ detail | name | summary ] list_name [ | { grep
grep_options | more ]
```

detail

Displays detailed information for the named prefix list.

name

Displays information for the named prefix list.

summary

Displays summary information for the named prefix list.

list_name

Specifies the name of an existing prefix list 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

Use this command to display information about IP prefix lists.

Example

To display detailed information about a prefix list named *route_101*, enter the following command:

```
show ip prefix-list detail route_101
```

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

show ip route

Displays information related to currently configured static or VRF routes 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 ip route [ ip_address/mask | vrf vrf_name ] [ | { grep grep_options | more
]
```

ip_address/mask

Specifies an IP address/mask (CIDR) for a static route in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

| vrf *vrf_name*

Displays information for an existing Virtual Routing and Forwarding (VRF) name expressed 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 display information related to currently configured static or VRF routes for the current context.

Example

To display detailed information about a route for a static IP address, enter the following command:

```
show ip route 10.1.0.0/24
```

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

show ip route-access-list

Displays information related to currently configured route-access-list used to filter routes.

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 ip route-access list [ name] [ | { grep grep_options | more ]
```

name

Specifies the name of an existing route access list 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

Use this command to display information about IP route access lists.

Example

To display detailed information about an access list named *access_route_3*, enter the following command:

```
show ip route-access-list accesss_route_3
```

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

show ip static-route

Displays information related to currently configured static routes.

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 ip static route [ ip_address/mask ] | { grep grep_options | more ]
```

ip_address/mask

Specifies an IP address/mask (CIDR) for a static route in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal 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 **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 about IP static routes.

Example

To display detailed information about route *192.155.33.2/24*, enter the following command:

```
show ip static route 192.155.33.2/24
```

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

show ip vrf

Displays configuration information for VPN Routing and Forwarding instances.

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

In 21.20.19 and earlier releases:

```
show ip vrf [ vrf_name [ mpls-map-dscp-exp ] ] ] | { grep grep_options | more
 ]
```

In 21.20.19 21.24 and later releases:

```
show ip vrf [ name vrf_name [ mpls-map-dscp-exp ] ] ] | { grep grep_options
| more ]
```

vrf_name

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

mpls-map-dscp-exp

Displays the MPLS mapping for the VRF.

Usage Guidelines

Use this command to display information about VRF names.

Example

To display information for a VRF named *corporate_range2* with MPLS mapping:

```
show ip vrf name corporate_range2 mpls-map-dscp-exp
```

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

show ip vrf-list

Displays configuration information for VRF lists currently 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 ip vrf-list [ list_name ]
```

list_name

Specifies the name of an existing VRF list as an alphanumerical string of 1 through 63 characters.

Usage Guidelines Use this command to display information about all VRF lists or a specified VRF list.

Example

The following command displays information about all VRF lists in the system:

```
show ip vrf-list
```

show ipms status

Displays the status of Intelligent Packet Monitoring System (IPMS) client service with information related to system and call events. It also displays the status of configured IPMS servers.

Product IPMS

Privilege Security Administrator, Administrator, Operator, Inspector

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show ipms status [ summary | all | server address ip_address ]
```

summary

Displays the summary of all configured IPMS client and IPMS servers.

all

Displays information for all configured IPMS client and IPMS servers.

server address *ip_address*

Displays status for the IPMS server specified as an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Usage Guidelines

This command is used to show/verify the status or configuration of one or all IPMS server along with system and call event information.

Example

The following command displays status of an IPMS server with IP address *10.2.3.4*:

```
show ipms status server address 10.2.3.4
```

show ipne peers

Generates a list of the IP Network Enabler (IPNE) peers.

Product

MME.

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show ipne peers { all | service ipne_service_name | summary } [ | { grep
grep_options | more } ]
```

all

Generates a list of all peers bound to the IPNE services, including the local and peer addresses. Also displays the TCP connections for every Session Manager.

service *ipne_service_name*

Generates a list of the peers associated with the specified IPNE service.

Summary

Generates a summary of all available IPNE peer 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 monitor and troubleshoot MME connections to the IPNE client and peer.

Example

List all IPNE peers with a command similar to the following:

```
show ipne peers all
```

show ipsg service

Displays IP Service Gateway (IPSG) service information.

Product

eWAG

IPSG

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show ipsg service { all | name ipsg_service_name } [ counters ][ | { grep
grep_options | more } ]
```

all

Displays information for all IPSG service(s) configured on the system.

name *ipsg_service_name*

Displays information for the specified IPSG service. *ipsg_service_name* must be an alphanumeric string of 1 through 63 characters.

counters

counters requires the output is to display counters associated with the IPSG service(s).

| { grep *grep_options* | more }

Specifies to pipe (send) the output of this command to the specified command. You must specify a command to which the output of this command should 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 IPSG services or a specific IPSG service.

Example

The following command displays information for all IPSG services configured on the system:

```
show ipsg service all
```

show ipsg sessions

Displays IP Service Gateway (IPSG) session information.

Product

eWAG

IPSG

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show ipsg sessions [ counters | full | summary ] [ all | callid call_id |
ip-address ipv4_address | msid msid_number | peer-address ipv4_address | username
 user_name ] [ | { grep grep_options | more } ]
```

counters

Displays session counters for matching sessions.

full

Displays all available information for matching sessions.

summary

Displays a summary of available information for matching sessions.

all

Displays session information including call ID, NAI, and home address for all current IPSG sessions.

This is the default behavior for the **show ipsg sessions** command.

callid *call_id*

Displays session information for a current IPSG session based on the specified call ID.

call_id must be an 8-digit hexadecimal number.

ip-address *ipv4_address*

Displays session information for a specific IPSG session based on the subscriber IP address.

ipv4_address must be specified in IPv4 dotted-decimal notation.

msid *msid_number*

Displays session information for a current IPSG session based on the specified MSID.

msid_number must be an 8-digit hexadecimal number.

peer-address *ipv4_address*

Displays session information for a current IPSG session based on the IP address of the device sending the RADIUS accounting messages.

ipv4_address must be specified in IPv4 dotted-decimal notation.

username *user_name*

Displays session information for an IPSG session based on subscriber's user name.

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 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 IPSG session information.

Example

The following command displays all the existing IPSG service sessions on the system:

```
show ipsg session all
```

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

show ipsg statistics

Displays IP Services Gateway (IPSG) service statistics.

Product

eWAG

IPSG

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

```
show ipsg statistics [ name ipsg_service_name | peer-address ipv4_address ] [
| { grep grep_options | more } ]
```

name *ipsg_service_name*

Displays cumulative statistics of all IPSG sessions processed by the specified service since the last system restart or clear command.

ipsg_service_name must be the name of an IPSG service, and must be an alphanumeric string of 1 through 63 characters.

peer-address *ipv4_address*

Displays cumulative statistics of all IPSG sessions associated with the specified IP address of the device sending the RADIUS accounting messages. The statistics displayed are from the last system restart or clear command.

ipv4_address must be specified in IPv4 dotted-decimal 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 **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 IPSG service statistics.

Example

The following command displays cumulative IPSG session statistics on the system:

```
show ipsg statistics
```

The following command displays the cumulative IPSG session statistics for an IPSG service named *ipsg1*:

```
show ipsg statistics name ipsg1
```

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

show ipv6 access-group statistics

Displays statistics for each rule in all IPv6 access groups or a specified IPv6 access control group.

Product

HA

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

```
show ipv6 access-group statistics [ | { 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 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 configured IPv6 access control groups in the current context.

Example

The following command displays the contents of an IPv6 access control group named *ACGv6_4*:

```
show ipv6 access-group ACGv6_4
```

show ipv6 access-list

Displays the information for all IPv6 Access Control Lists (ACLs) or the named ACL. With no keyword supplied, a list of all access lists and their entries is displayed.

Product

HA

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

```
show ipv6 access-list list_name [ | { grep grep_options | more } ]
```

list_name

Specifies the name of an existing ACL configured in the current context as an alphanumeric string of 1 through 47 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 the configured IPv6 ACLs in the current context.

Example

The following command displays the contents of an IPv6 ACL named *ACLv6_4*:

```
show ipv6 access-list ACLv6_4
```

show ipv6 interface

Displays statistical and configuration information for the IPv6-based interfaces, including a Virtual Routing and Forwarding (VRF) table for a specific 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 ipv6 interface [ name intfc_name ] [ statistics ] [ summary ] [ vrf
vrf-name ] [ | { grep grep_options | more } ]
```

name *intfc_name*

Displays information for an existing interface specified as an alphanumeric string of 1 through 79 characters. If no interface name is specified, the information for all IPv6 interfaces is displayed.

statistics

Displays the session statistics of all ingress and egress packets processed through this IPv6 interface.

summary

Displays summarized information about requested IPv6 interfaces.

vrf *vrf_name*

Displays Virtual Routing and Forwarding (VRF) routing information for an existing VRF 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 display the summarized of detailed configuration and statistical information for a configured IPv6 interface. This information can be used to verify and/or troubleshoot communication difficulties between to a remote host/node.

Example

The following command displays the interface information, including statistics, for the IPv6 interface *IPv6Interface_2*.

```
show ipv6 interface IPv6Interface_2 statistics
```

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

show ipv6 neighbors

Displays the neighbor table for all IPv6 addresses or a specified IPv6 address in 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 ipv6 neighbors [ ipv6_address ] [ vrf vrf-name  ] [ | { grep grep_options
| more } ]
```

ipv6_address

Displays information for an existing IPv6 address specified in IPv6 colon-separated-hexadecimal notation. If no IPv6 address is specified, the information for all IPv6 addresses is displayed.

vrf *vrf_name*

Displays Virtual Routing and Forwarding (VRF) routing information for an existing VRF 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 display neighbor information for IPv6 address(es) in the current context. This information can be used to verify and/or troubleshoot communication difficulties between to a remote host/node.

Example

The following command displays the neighbor information for the IPv6 address *ffe:ffff:101::230:6eff:fe04:d9aa*.

```
show ipv6 neighbor ffe:ffff:101::230:6eff:fe04:d9aa
```

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

show ipv6 ospf

Displays information regarding the configuration of the OSPFv3 Protocol on this system.

Product

PDSN

HA

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 ipv6 ospf [ database | debugging | interface | nieghbor | route |
virtual-links ] [ verbose [ verbose ] [ | { grep grep_options | more } ]
show ipv6 ospf database [ adv-routeripv4-address  ] [ ls-type { external |
inter-prefix  | inter-router | intra-prefix | link | network | router }
show ipv6 ospf debugging
show ipv6 ospf interface
show ipv6 ospf neighbor [ details]
show ipv6 ospf route [ summary ]
show ipv6 ospf virtual-links
```

show ipv6 ospf database

Displays the OSPFv3 database including the following components.

- **adv-router** *ipv4-address*: Displays OSPF database information from the advertising router specified as an IP address in IPv4 dotted-decimal notation.
- **ls-type**: Displays the specified Link-State Advertisement (LSA) type, which can be one of the following:
    - **external**: Display External LSA information
    - **inter-prefix**: Displays Inter Area Prefix LSA information
    - **inter-router**: Displays Inter Area Router LSA information
    - **intra-prefix**: Displays Intra Area Prefix LSA information
    - **link**: Displays Link LSA information
    - **network**: Displays Network LSA information
    - **router**: Displays Router LSA information

show ipv6 ospf debugging

Displays OSPFv3 Debugging Flags.

show ipv6 ospf interface

Displays OSPFv3 Interfaces.

show ipv6 ospf neighbor [details]

Displays OSPFv3 neighbors with the option for full details.

show ipv6 ospf route [summary]

Displays OSPFv3 route information with the option for summarized information.

show ipv6 ospf virtual-links

Displays OSPFv3 virtual links.

verbose

Displays detailed 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

Use this command to see all OSPFv3 information.

Example

The following command displays IPv6 OSPF information:

```
show ipv6 ospf
```

show ipv6 pool

Displays information related IPv6 Pool configuration/state.

Product

PDSN

GGSN

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 ipv6 pool[ group-name group-name ] [ pool-name pool-name ] [ summary ] [
verbose ] [ | { grep grep_options | more } ]
```

group-name*group-name*

Displays IP address pool information for an existing group-name specified as an alphanumeric string of 1 through 31 characters.

pool-name *pool-name*

Displays IPv6 address pool information for an existing pool name specified as an alphanumeric string of 1 through 31 characters.

summary

Displays summary information about all IP address pools; this is the default.

verbose

Displays detailed information about all IP address pools.

| { 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 see all the ipv6 pool information.

Example

The following command displays IPv6 pool information:

```
show ipv6 pool
```

show ipv6 prefix-list

Displays information related to an IPv6 prefix list.

Product

PDSN

GGSN

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 ipv6 prefix-list[ detailprefix-list-name ] [ nameprefix-list-name [
ip-address/mask [ longer ] [ match-first ] ] [ seq seq_value ] ] [ summary
prefix-list-name] [ | { grep grep_options | more } ]
```

detail*prefix-list-name*

Displays detailed IP address information for an existing prefix-list specified as an alphanumeric string of 1 through 79 characters.

name*prefix-list-name*

Displays IP address information for an existing prefix-list specified as an alphanumeric string of 1 through 79 characters.

ip-address/mask

Specifies an IPv6 Network Address/Mask Bits combination in CIDR notation.

longer

Displays IP address prefix-list details in longer format.

match-first

Displays first matched IP address prefix-list details.

seq *seq_value*

Specifies the sequence number as an integer from 1 through 4294967295.

seq_value is the integer value between 1 through 4294967295.

summary *prefix-list-name*

Displays prefix-list summary for an existing prefix-list 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

Use this command to see all the ipv6 prefix-list information.

Example

The following command displays IPv6 prefix list information:

```
show ipv6 prefix-list
```

show ipv6 route

Displays information related to specific route for current context.

Product

PDSN

GGSN

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 ipv6 route [ ip-address/mask ] [ vrf vrf-name ] [ | { grep grep_options | more } ]
```

ip-address/mask

Specifies an IP address entered using IPv6 colon-separated-hexadecimal and CIDR notation.

vrf *vrf-name*

Displays Virtual Routing and Forwarding (VRF) routing information for an existing VRF 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 see all the ipv6 route information.

Example

The following command displays IPv6 route information:

```
show ipv6 route 2001:0db8:85a3:0000:0000:8a2e:0370:7334/5
```

show ipv6 route-access-list

Displays the route access list.

Product

PDSN

GGSN

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 ipv6 route-access-list [ route-access-list ] [ | { grep grep_options | more } ]
```

route-access-list

route-access-list is 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

Use this command to see all the IPv6 route access list information.

Example

The following command displays IPv6 route access list information:

```
show ipv6 route-access-list
```

show iups-service

Displays information for Iu-PS services in the current context. The Iu-PS interface links the radio network controller (RNC) with the packet switched core network.

Product

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 iups-service { all | name srvc_name} [ gtpu-table | rnc { all | id
rnc_id } ] [ | { grep grep_options | more } ]
```

all

Shows information for all configured IuPS services.

name *srvc_name*

Specifies an existing IuPS service as an alphanumeric string of 1 through 63 characters.

gtpu-table

Displays the configured GTPU database.

rnc all

Displays information for all configured RNCs.

rnc ***rnc_id***

Specifies the identification number of an existing RNC configuration instance as an integer from 0 through 4095.

| { 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

Iu-PS services control the interface between the SGSN and the RNCs in the UMTS radio access network (UTRAN). Iu-PS services include the control plane and the data plane between these nodes.

Use this command to display information for a specific Iu-PS service or for all Iu-PS services configured within the context. A filtering keyword can limit the display to only information for a specific RNC or for a GTPU table in the Iu-PS service configuration.

Example

The next command displays information for all Iu-PS services configured in the current context:

```
show iups-service all
```

This command displays information for a specific RNC for a specific Iu-PS services:

```
show iups-service name iups-svc-1 rnc 123name
```

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

show l2tp sessions

Displays information for Layer 2 Tunneling Protocol (L2TP) tunnels.

Product

LNS

PDSN

GGSN

HA

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show l2tp sessions [ full | summary | counters ] [ all | callid id | username name | msid ms_id | lac-service service_name | lns-service service_name | pdsnclosedrp-service service_name | peer-address [ operator ] peer_address ]
```

full

Displays all available information for the specified sessions.

summary

Displays a summary of available information for the specified sessions.

counters

Displays counters for the specified L2TP sessions.

all

Displays all current sessions.

callid *id*

Displays session information for the call ID. specified an 8-byte hexadecimal number. The output of the command **show l2tp tunnels** contains a field labeled Callid Hint which lists the call ID information to use with this command.

username *name*

Displays session information for an existing subscriber specified as an alphanumeric string of 1 through 127 characters. Wildcard characters $ and * are allowed.

msid *ms_id*

Displays session information for the MSID specified as 7 to 16 digits for an IMSI, MIN, or RMI. Wildcard characters $ and * are allowed.

lac-service *service_name*

Displays all L2TP sessions in the specified LAC service.

lns-service *service_name*

Displays all L2TP sessions in the specified LNS service.

pdsnclosedrp-service *service_name*

Displays all L2TP sessions in the specified Closed R-P service.

peer-address [*operator*] *peer_address*

Displays all L2TP sessions to the destination (peer LNS) specified as an IP address in IPv4 dotted-decimal notation.

In conjunction with **sessions** keyword, indicates a range of peers is to be displayed.

peer-address [*operator*] *peer_address* is specified using IPv4 dotted-decimal notation.

operator implies how to logically specify a range of peer-address and it must be one of the following:

- <: IP address less than the specified *peer_address*
- >: IP address less than the specified *peer_address*
- **greater-than**: IP address less than the specified *peer_address*
- **less-than**: IP address less than the specified *peer_address*

Usage Guidelines

Use this command to show information for sessions in the current context.

Important If this command is executed from within the local context, cumulative session information is displayed for all contexts.

Example

The following command displays cumulative statistics for all sessions processed within the current context:

```
show l2tp sessions
```

The following command displays all information pertaining to the L2TP session of a subscriber named *isp1vpnuser1*:

```
show l2tp session full username isp1vpnuser1
```

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

show l2tp statistics

Displays statistics for all Layer 2 Tunneling Protocol (L2TP) tunnels and sessions.

Product

PDSN

GGSN

HA

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show l2tp statistics [lac-service *service_name* **| lns-service** *service_name* **| pdsnclosedrp-service** *service_name* **| peer-address** *peer_ip_address* **]**

lac-service *service_name*

Displays L2TP statistics for all tunnels and sessions in an existing L2TP Access Concentrator (LAC) service specified as an alphanumeric string of 1 through 63 characters.

lns-service *service_name*

Displays L2TP statistics for all tunnels and sessions in tan existing L2TP Network Server (LNS) service specified as an alphanumeric string of 1 through 63 characters.

pdsnclosedrp-service *service_name*

Displays L2TP statistics for all tunnels and sessions in an existing Closed R-P service specified as an alphanumeric string of 1 through 63 characters.

peer-address *peer_address*

Displays L2TP statistics for all tunnels and sessions to the destination (peer LNS) at the IP address specified in IPv4 dotted-decimal notation.

Usage Guidelines

Use this command to display statistics for L2TP services.

Example

The following command displays statistics for a specific LAC service named *vpn1*:

```
show l2tp statistics lac-service vpn1
```

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

show l2tp tunnels

Displays information for Layer 2 Tunneling Protocol (L2TP) tunnels.

Product

PDSN

GGSN

HA

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]`*`host_name`*`#`

Syntax Description

```
show l2tp tunnels [ full | summary | counters ] [ all | callid id |
username name | msid ms_id | lac-service service_name | lns-service service_name
 | pdsnclosedrp-service service_name | peer-address [ operator ] peer_address
]
```

full

Displays all available information for the specified tunnels.

summary

Displays a summary of available information for the specified tunnels.

counters

Displays counters for the specified L2TP tunnels.

all

Displays all current tunnels.

callid *id*

Displays tunnel information for the call id specified as an 8-digit hexadecimal number. The output of the command **show l2tp tunnels** contains a field labeled Callid Hint which lists the call id information to use with this command.

username *name*

Displays tunnel information for an existing subscriber specified as an alphanumeric string of 1 through 127 characters. Wildcard characters $ and * are allowed.

msid *ms_id*

Displays tunnel information for the MSID specified as 7 to 16 digits for an IMSI, MIN, or RMI. Wildcard characters $ and * are allowed.

lac-service *service_name*

Displays all L2TP tunnels in the specified LAC service.

lns-service *service_name*

Displays all L2TP tunnels in the specified LNS service.

pdsnclosedrp-service *service_name*

Displays all L2TP tunnels in the specified Closed R-P service.

peer-address [*operator*] *peer_address*

Displays all L2TP tunnels to the destination (peer LNS) at the IP address specified in IPv4 dotted-decimal notation.

In conjunction with **tunnels** keyword, indicates a range of peers is to be displayed.

peer-address [*operator*]: Specifies a peer address using IPv4 dotted-decimal notation.

operator implies how to logically specify a range of peer-address and it must be one of the following:

- <: IP address less than the specified *peer_address*
- >: IP address less than the specified *peer_address*
- **greater-than**: IP address less than the specified *peer_address*
- **less-than**: IP address less than the specified *peer_address*

Usage Guidelines

Use this command to show information for tunnels in the current context.

Example

The following command displays all of the tunnels currently being facilitated by LAC services within the current context:

```
show l2tp tunnels all
```

The following command displays information pertaining to the L2TP tunnel(s) established for a LAC-service named vpn1:

```
show l2tp tunnels full lac-service vpn1
```

Important

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

show lac-service

Displays the information for all L2TP Access Concentrator (LAC) services or for a particular LAC service.

Product

PDSN

HA

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 lac-service { all | name service_name } [ | { grep grep_options | more }
 ]
```

all

Display information for all LAC services.

name *service_name*

Display information only for an existing LAC 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

Use this command to list information for LAC services configured on this system.

Example

The following commands display information for all LAC services and the LAC service named *lac1*, respectively.

```
show lac-service all
```

```
show lac-service name lac1
```

show lawful-intercept

Refer to the *Lawful Intercept Configuration Guide* for a full description of this command.

show lawful-intercept ssdf statistics

Refer to the *Lawful Intercept Configuration Guide* for a description of these statistics.

show ldap connection all

Displays all details about the Lightweight Directory Access Protocol (LDAP) subsystem.

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 ldap connection all   [ | { 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 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

Display all details about the LDAP subsystem.

Example

The following command displays full information about the LDAP subsystem.

```
show ldap connection all
```

show leds

Displays the current status of the light emitting diodes (LEDs) for a specific card or all cards.

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 leds { all | card_num } [ | { grep grep_options | more } ]
```

all | *card_num*

all: Displays the LED status for all cards.

card_num: Displays the LED status for the card specified by its slot number.

| { 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

Display the status of the LEDs as a part of an automated periodic script which checks the LEDs of the chassis.

Important

This command is not supported on all platforms.

Example

The following commands display the LED status for all cards and only card *8*, respectively.

```
show leds all
```

```
show leds 8
```

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

show license

Displays information about licensing as configured on this system.

Product

All

Privilege

Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show license { all | enforcement { policy | status [ allowed | blocked ]
 [ feature | service ] } | eval-period | history | information [ key
key_name ] [ full ] | key | privilege-bits | smart-tags [ feature | service
 ] | statistics [ verbose ] | status | summary | tech-support | udi |
usage } [ | { grep grep_options | more } ]
```

all

Shows a superset of information that includes show status, show usage, show UDI, as well as the Smart Licensing agent version.

This keyword applies to Smart Licensing only.

enforcement { policy | status [allowed | blocked] [feature | service] }

Shows the enforcement policy applied to or current enforcement status of Smart Licenses. Status information can be filtered based on the licenses which are currently allowed or blocked, or by license type.

allowed: displays the current status, and if out of compliance (OOC) the list of services which are blocked.

blocked: displays the list of services and features which are blocked.

feature: displays the current status, and if out of compliance (OOC) the list of services which are blocked.

service: displays the current status and if out of compliance (OOC) the list of services and features which are blocked.

This keyword applies to Smart Licensing only.

eval-period

Shows information about the evaluation period. Licenses are granted a 90 day evaluation period until they are registered.

This keyword applies to Smart Licensing only.

history

Displays the history of installed license and how much time each license was in each state. This keyword applies to legacy licensing only.

information [key *key_name*] [full]

Displays the license information to verify the proper keys have been installed. This command is also helpful in troubleshooting user system access due to the maximum number of sessions being reached.

key *key_name*: Displays the information for an existing license key specified as an alphanumeric string of 1 of 1 through 500 characters.

full: Displays the full features and quantities without any hardware limits in place.

key

Displays the installed keys in encrypted format.

privilege-bits

Displays all the CLI privilege bits that are turned on. This keyword applies for legacy licensing only.

smart-tags [feature | service]

Shows the features and services that are currently supported and the corresponding Smart Entitlement Tags.

feature: filters the output to show only features.

service: filters the output to show only services.

This keyword applies to Smart Licensing only.

statistics [verbose]

Shows Smart Licensing details for each individual feature. Use the optional **verbose** keyword to display additional information.

status

Shows information about the current state of Smart Licensing on the system, such as registration and license authorization status.

summary

Shows information about the current state of Smart Licensing on the system, such as registration, license authorization, and license usage status.

tech-support

Shows information useful for debugging issues with Smart Licensing.

udi

Shows details for all Unique Device Identifiers (UDI). This keyword applies to Smart Licensing only.

usage

Shows the usage information for all entitlements that are currently in use. This keyword applies to Smart Licensing only.

| { 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 licensing information, both the legacy licensing model as well as the Smart Licensing model introduced in Release 21.3. The history, information, key, and privilege-bits keywords apply only to the legacy license key model. All other keywords display information related to Smart Licensing introduced in Release 21.3.

Refer to the *Smart Licensing* chapter of the *System Administration Guide* for more details about Smart Licensing.

Example

The following displays all information about Smart Licensing as configured on the system.

```
show license all
```

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

show link-aggregation

Displays information about any Link Aggregation Group (LAG) configured in this system. A LAG works by exchanging control packets via Link Aggregation Control Protocol (LACP) over configured physical ports with peers to reach agreement on an aggregation of links. The LAG sends and receives the control packets directly on physical ports.

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 link-aggregation { info | lacp info | statistics } group group_number
[ | { grep grep_options | more } ]
show link-aggregation table [all] [ | { grep grep_options | more } ]
show link-aggregation utilization table [ | { grep grep_options | more } ]
```

{ info | lacp info | statistics }

Displays the following categories of LAG information:

- **info** – LAG configuration and operating state
- **lacp info** – LACP Rx and Tx counters
- **statistics** – LAG Rx and Tx counters and data throughput statistics

group *group_number*

Specifies the LAG number as an integer from 1 through 1023.

table [all] *group_number*

Displays information about the current LAG port configuration in tabular form. The **all** option includes ATM PVCs for ATM ports (ASR 5000 only).

utilization table

Displays LAG utilization data in tabular form.

| { 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 information about any Link Aggregation Group (LAG) configured in this system.

Example

The following command displays configuration information for LAG number 100:

show link-aggregation info group 100

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

show linkmgr

Displays statistics for the link manager (linkmgr).

Product

SGSN

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

```
show linkmgr { all | instance instance } [ parser | | ]
```

all

Display statistics for all link managers.

instance *instance*

Display statistics for a single instance of a link manager specified as an integer from 1 to 4.

| { 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 statistical information for the SGSN's link manager which handles the layer between the session manager and the SS7 functionality downwards from layer 3.

Example

Use the following command to display the statistics for link manager *4*:

```
show linkmgr 4
```

Important

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

show llc statistics

Displays traffic statistics for the GPRS logical link-control (LLC) layer.

Product

SGSN

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show llc statistics [ gprs-service srvc_name ] [ verbose ] [ | { grep grep_options | more } ]
```

gprs-service *srvc_name*

Displays the statistics for an existing GPRS service specified as an alphanumeric string of 1 through 63 characters.

verbose

Displays all possible statistics for specified command or 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 more information on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference*.

Usage Guidelines

This command can display either a summarized or full (verbose) view of statistics collected for the traffic that has gone through the LLC layer for either all GPRS services or for a specified GPRS service.

Example

The following command displays the frame Tx/Rx LLC statistics for GPRS service *gprs1*:

```
show llc statistics gprs-service gprs1
```

show llc status

Displays status information for the GPRS logical link-control (LLC) layer.

Product

SGSN

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show llc status gprs-service srvc_name sessmgr instance instance { dlci ms-id
 ms_id sapi sapid | lsap sapid sapid | ms ms_id | usap sapid sapid [ | { grep
 grep_options | more } ]
```

gprs-service *srvc_name*

Displays the LLC layer status for an existing GPRS service specified as an alphanumeric string of 1 through 63 characters.

sessmgr instance *instance*

Displays the LLC status for a session manager instance specified as an integer. The range varies depending upon the release:

- for releases prior to 14.0, the range is from 1 to 4294967295.
- for releases 14.0 and later, the range is from 1 to 384.

dlci ms-id *ms_id* [sapi *sapid*]

Displays the LLC status for a specific data link connection identifier (DLCI) between the LLC and the mobile station (MS). *ms_id* must be an integer from 0 to 65536 that identifies the DLCI interface connecting to a specific MS.

sapi: Filters the display of the LLC status information to focus on a specific service access point interface (SAPI) within the specified DLCI specified as.an integer from 1 to 11

lsap *sapid*

Refines the display of the LLC status to focus on a specific lower service access point interface (LSAP) specified as an integer from 0 to 65536.

ms-id *ms_id*

Displays the LLC status for a connected MS specified as an integer from 0 to 65536.

usap *sapid*

Refines the display of the LLC statistics to focus on a specific upper service access point interface (USAP) specified as an integer from 0 to 65536.

| { 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 to the *Regulating a Command's Output* section of the *Command Line Interface Reference*.

Usage Guidelines

This command can display either a summarized or full (verbose) view of statistics collected for the traffic that has gone through the LLC layer for either all GPRS services or for a specified GPRS service.

Example

The following command displays the frame Tx/Rx LLC statistics for GPRS service *gprs1*:

```
show llc statistics gprs-service gprs1
```

show lma-service

Displays statistic and counter information for Local Mobility Anchor (LMA) services on this system.

Product

P-GW

SAEGW

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show lma-service all
show lma-service name service_name
show lma-service session [ all | callid id | counters | full | ipv6-address
 { < address | > address | address | greater-than address [ less-than address ]
 | less-than address [ greater-than address ] } | summary | username name ]
show lma-service statistics [ lma-service name ] } [ | { grep grep_options
| more } ]
```

all

Displays information about all configured LMA services on this system.

name *service_name*

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

session [all | callid *id* | counters | full | ipv6-address { < *address* | > *address* | *address* | greater-than *address* [less-than *address*] | less-than *address* [greater-than *address*] } | summary | username *name*]

Displays session information filtered by the following parameters:

all: Displays all active LMA sessions using LMA services on the system.

callid *id*: Displays available session information for the call identification number specified as an eight-byte hexadecimal number.

counters: Displays session counters for active LMA sessions using LMA services on the system. This keyword can also be filtered by the following:

- **all**

- **callid**
- **ipv6-address**
- **username**

Refer to the keyword descriptions in this command for information regarding these filters.

full: Displays additional session information for active LMA sessions using LMA services on the system. This keyword includes the information in the output of the **all** keyword plus additional information. This keyword can also be filtered by the following:

- **all**
- **callid**
- **ipv6-address**
- **username**

Refer to the keyword descriptions in this command for information regarding these filters.

ipv6-address:

- < *address* and **less-than** *address*: Displays summarized information for a group of IPv6 addresses that are less than the specified IPv6 address using one of these keywords. A range can be specified by including an address with the **greater-than** option. *address* must be specified in IPv6 colon-separated-hexadecimal notation.
- > *address* and **greater-than** *address*: Displays summarized information for a group of IPv6 addresses that are greater than the specified IPv6 address using one of these keywords. A range can be specified by including an address with the **less-than** option. *address* must be specified in IPv6 colon-separated-hexadecimal notation.
- *address*: Displays summarized information for a specific IPv6 address using an LMA service on this system. *address* must be specified in IPv6 colon-separated-hexadecimal notation.

summary: Displays the number of LMA sessions currently active for LMA services configured on the system.

username *name*: Displays available session information for an existing user specified as an alphanumeric string of 1 through 127 characters.

statistics [lma-service *name*]

lma-service *name*: Displays LMA service statistics for an existing LMA 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 the **grep** and **more** commands, 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 LMA services on this system.

Example

The following command displays service statistics for the LMA service named *lma1*:

```
show lma-service name lma1
```

show lns-service

Displays the information for all L2TP Network Server (LNS) services or for a particular LNS service.

Product

PDSN

HA

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 lns-service { all | name service_name } [ | { grep grep_options | more } ]
```

all

Display information for all LNS services.

name *service_name*

Displays information only for an existing LNS 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

Use this command to list information for LNS services configured on this system.

Example

The following commands display information for all LNS services and the LNS service named *lns1*, respectively.

```
show lns-service all
show lns-service name lns1
```

show local-policy

Displays information pertaining to local QoS policy services.

Product

P-GW

SAEGW

Privilege

Security Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show local-policy statistics { all | service service_name | summary } | { grep grep_options | more }
```

statistics { all | service *service_name* | summary }

Display statistics pertaining to local QoS services.

all: Displays information for all local QoS services.

service *service_name*: Displays statistics only for an existing local QoS service specified as an alphanumeric string of 1 through 64 characters.

summary: Displays summarized statistics all local QoS 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 statistics for local QoS policies on this system.

Example

The following command displays statistics for the local QoS policy named *sample1*.

show local-policy statistics service sample1

show local-user

Displays information pertaining to local-user accounts.

Important In a release 20.0 or higher Trusted build, this command is not available.

Product All

Privilege Security Administrator

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show local-user [ [ username name ] [ inactive filter ] [ verbose | wide ]
 | statistics [ verbose ] ]
```

username *name*

Displays information for an existing local-user administrative account specified as an alphanumeric string of 3 through 16 characters that is case sensitive. If a username is not specified, information is displayed for all local users.

inactive *filter*

Specifies a filter for displaying inactive local-user accounts:

- < *days*: Displays accounts that have been inactive less than the specified number of days.
- > *days*: Displays accounts that have been inactive more than the specified number of days.
- **greater-than** *days*: Displays accounts that have been inactive more than the specified number of days.
- **less-than** *days*: Displays accounts that have been inactive less than the specified number of days.

days can be configured to an integer from 1 through 365.

[verbose | wide]

Specifies how the information is to be displayed as one of the following options:

- **verbose**: The data is displayed in list format. Additional information is provided beyond what is displayed when the **wide** option is used.
- **wide**: The data is displayed in tabular format. This is the default setting.

statistics [verbose]

Displays local-user statistics.

Using the **verbose** keyword displays additional statistics.

Usage Guidelines Use this command to display information and statistics on local-user administrative accounts.

Example

The following command displays detailed information on local-user administrative accounts that have been inactive for more than 10 days:

```
show local-user inactive greater-than 10 verbose
```

The following command displays detailed information for a local-user account named *Test*:

```
show local-user username Test verbose
```

The following command displays detailed local-user account statistics:

```
show local-user statistics verbose
```

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

show location-service

Displays information and statistics for all location services or for a specific location service.

Product MME

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 location-service { service { all | name service_name } | statistics {
 all | service service_name } [ | { grep grep_options | more } ]
```

service { all | name *service_name* }

Display configuration information pertaining to location services.

all: Displays information for all location services.

name *service_name*: Displays information only for an existing location service specified as an alphanumeric string of 1 through 63 characters.

statistics { all | service *service_name* }

Display statistics pertaining to location services.

all: Displays statistics for all location services.

name *service_name*: Displays statistics only for an existing location service 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 list configuration information and statistics for location services configured on this system.

Example

The following commands display information for all location services and the location service named *location_service1*, respectively.

```
show location-service service all
```

```
show location-service service name location_service1
```

The following command displays statistics for the location service named *location_service1*.

```
show location-service statistics service location_service1
```

show logging

Displays the defined logging filters 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 logging [ active | verbose ] [ | { grep grep_options | more } ]
```

active | verbose

active: Displays only active CLI logging filter information in concise format.

verbose: Displays as much information as possible.

| { 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 log filters to troubleshoot disk utilization issues.

Example

```
show logging
show logging active
show logging verbose
show logging active verbose
```

show logical-port utilization table

Displays logical port (VLAN and NPU) utilization for a specified interface port.

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 logical port utilization table slot/port [vlan { 5-minute | hourly }]
 [ | { grep grep_options | more } ]
```

slot/port

Specifies the port for which logical-port statistics will be displayed. The slot and port must refer to an installed card and port.

vlan { 5-minute | hourly }

Displays only active VLAN information for the specified collection interval.

- **5-minute**: Displays 5-minute utilization intervals for the past 24 hours.
- **hourly**: Displays hourly utilization intervals for the past 24 hours.

| { 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 logical port (VLAN) statistics for 5-minute intervals on port 17/1.

Example

```
show logical-port utilization table 17/1 vlan 5-minute
```

show logs

Displays active and inactive logs filtered by the options specified.

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 logs [ active ] [ inactive ] [ callid call_id ] [ encrypted-li ] [
event-verbosity evt_verboseness ] [ facility facility ] [ level severity_level
] [ pdu-data pdu_format ] [ pdu-verbosity pdu_verboseness ] [ proclet facility
] [ since from_date_time [ until to_date_time ] ] [ | { grep grep_options | more
 } ]
```

active

Displays data from active logs.

inactive

Displays data from inactive logs.

callid *call_id*

Displays log information only for a call ID specified as a 4-digit hexadecimal number.

encrypted-li

This keyword is only visible to an administrator with li-privilege. It displays the boot config output for the encrypted LI configuration when **require segregated li-configuration** has been enabled.

Note For additional information, see the *Lawful Intercept Configuration Guide*.

event-verbosity *evt_verboseness*

Specifies the level of verboseness to use in displaying of event data as one of:

- **min** - displays minimal information about the event. Information includes event name, facility, event ID, severity level, date, and time.

- **concise** - displays detailed information about the event, but does not provide the event source within the system.
- **full** - displays detailed information about event, including source information, identifying where within the system the event was generated.

facility *facility*

Specifies the facility to modify the filtering of logged information for as one of:

- **a10**: A10 interface facility
- **a11**: A11 interface facility
- **a11mgr**: A11 Manager facility
- **aaa-client**: Authentication, Authorization and Accounting (AAA) client facility
- **aaamgr**: AAA manager logging facility
- **aaaproxy**: AAA Proxy facility
- **aal2**: ATM Adaptation Layer 2 (AAL2) protocol logging facility
- **acl-log**: Access Control List (ACL) logging facility
- **acsctrl**: Active Charging Service (ACS) Controller facility
- **acsmgr**: ACS Manager facility
- **afctrl**: Fabric Controller facility [ASR 5500 only]
- **afmgr**: Fabric Manager logging facility [ASR 5500 only]
- **alarmctrl**: Alarm Controller facility
- **alcap**: Access Link Control Application Part (ALCAP) protocol logging facility
- **alcapmgr**: ALCAP manager logging facility
- **all**: All facilities
- **asngwmgr**: Access Service Network (ASN) Gateway Manager facility
- **asnpcmgr**: ASN Paging Controller Manager facility
- **bfd**: Bidirectional Forwarding Detection (BFD) protocol logging facility
- **bgp**: Border Gateway Protocol (BGP) facility
- **bindmux**: IPCF BindMux-Demux Manager logging facility
- **bngmgr**: Broadband Network Gateway (BNG) Demux Manager logging facility
- **bssap+**: Base Station Sub-system Application Part+ protocol facility for the login interface between the SGSN and the MSC/VLR (2.5G and 3G)
- **bssgp**: Base Station Sub-system GPRS Protocol logging facility handles exchange information between the SGSN and the BSS (2.5G only)
- **bulkstat**: Statistics logging facility

- **callhome**: Call Home application logging facility
- **cap**: CAMEL Application Part (CAP) logging facility for protocol used in prepaid applications (2.5G and 3G)
- **cbsmgr**: Cell Broadcasting Service (CBS) logging facility [HNBGW]

> **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.

- **cdf**: Charging Data Function (CDF) logging facility
- **cgw**: Converged Access Gateway (CGW) logging facility
- **cli**: Command Line Interface (CLI) logging facility
- **cmp**: Certificate Management Protocol (IPSec) logging facility
- **confdmgr**: ConfD Manager proclet (NETCONF) logging facility
- **connectedapps**: SecGW ASR 9000 oneP communication procotol
- **connproxy**: Controller Proxy logging facility
- **credit-control**: Credit Control (CC) facility
- **csp**: Card/Slot/Port controller facility
- **css**: Content Service Selection (CSS) facility
- **css-sig**: CSS RADIUS Signaling facility
- **cx-diameter**: Cx Diameter Messages facility [CSCF <--> HSS]
- **data-mgr**: Data Manager Framework logging facility
- **dcardctrl**: IPSec Daughter Card Controller logging facility
- **dcardmgr**: IPSec Daughter Card Manager logging facility
- **demuxmgr**: Demux Manager API facility
- **dgmbmgr**: Diameter Gmb Application Manager logging facility
- **dhcp**: Dynamic Host Configuration Protocol (DHCP) logging facility
- **dhcpv6**: DHCPv6
- **dhost**: Distributed Host logging facility
- **diabase**: Diabase messages facility
- **diactrl**: Diameter Controller proclet logging facility
- **diameter**: Diameter endpoint logging facility
- **diameter-acct**: Diameter Accounting

- **diameter-auth**: Diameter Authentication
- **diameter-dns**: Diameter DNS subsystem
- **diameter-ecs**: ACS Diameter signaling facility
- **diameter-engine**: Diameter version2 engine logging facility
- **diameter-hdd**: Diameter Horizontal Directional Drilling (HDD) Interface facility
- **diameter-svc**: Diameter Service
- **diamproxy**: DiamProxy logging facility
- **dpath**: IPSec Data Path facility
- **drvctrl**: Driver Controller facility
- **dpath**: IPSec Data Path logging facility
- **drvctrl**: Driver Controller logging facility
- **doulosuemgr**: Doulos (IMS-IPSec-Tool) user equipment manager
- **eap-diameter**: Extensible Authentication Protocol (EAP) IP Sec urity facility
- **eap-ipsec**: Extensible Authentication Protocol (EAP) IPSec facility
- **eap-sta-s6a-s13-s6b-diameter**: EAP/STA/S6A/S13/S6B Diameter messages facility
- **ecs-css**: ACSMGR <-> Session Manager Signalling Interface facility
- **egtpc**: eGTP-C logging facility
- **egtpmgr**: enhanced GPRS Tunneling Protocol (eGTP) manager logging facility
- **egtpu**: eGTP-U logging facility
- **embms**: evolved Multimedia Broadcast Multicast Services Gateway facility
- **embms**: eMBMS Gateway Demux facility
- **epdg**: evolved Packet Data (ePDG) gateway logging facility
- **event-notif**: Event Notification Interface logging facility
- **evlog**: Event log facility
- **famgr**: Foreign Agent manager logging facility
- **firewall**: Firewall logging facility
- **fng**: Femto Network Gateway (FNG) logging facility
- **gbmgr**: SGSN Gb Interface Manager facility
- **gmm**:
  - For 2.5G: Logs the GPRS Mobility Management (GMM) layer (above LLC layer)
  - For 3G: Logs the access application layer (above the RANAP layer)

- **gprs-app**: GPRS Application logging facility
- **gprs-ns**: GPRS Network Service Protocol (layer between SGSN and the BSS) logging facility
- **gq-rx-tx-diameter**: Gq/Rx/Tx Diameter messages facility
- **gss-gcdr**: GTPP Storage Server GCDR facility
- **gtpc**: GTP-C protocol logging facility
- **gtpcmgr**: GTP-C protocol manager logging facility
- **gtpp**: GTP-prime protocol logging facility
- **gtpu**: GTP-U protocol logging facility
- **gtpumgr**: GTP-U Demux manager
- **gx-ty-diameter**: Gx/Ty Diameter messages facility
- **gy-diameter**: Gy Diameter messages facility
- **h248prt**: H.248 port manager facility
- **hamgr**: Home Agent manager logging facility
- **hat**: High Availability Task (HAT) process facility
- **hdctrl**: HD Controller logging facility
- **henbapp**: Home Evolved NodeB (HENB) App facility

  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.

- **henbgw**: HENB-GW facility

  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.

- **henbgw-pws**: HENB-GW Public Warning System logging facility

  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.

- **henbgw-sctp-acs**: HENB-GW access Stream Control Transmission Protocol (SCTP) facility

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.

- **henbgw-sctp-nw**: HENBGW network SCTP facility

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.

- **henbgwdemux**: HENB-GW Demux facility

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.

- **henbgwmgr**: HENB-GW Manager facility

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.

- **hnb-gw**: HNB-GW (3G Femto GW) logging facility

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.

- **hnbmgr**: HNB-GW Demux Manager logging facility

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.

- **hss-peer-service**: Home Subscriber Server (HSS) Peer Service facility
- **igmp**: Internet Group Management Protocol (IGMP)
- **ikev2**: Internet Key Exchange version 2 (IKEv2)
- **ims-authorizatn**: IP Multimedia Subsystem (IMS) Authorization Service facility

- **ims-sh**: HSS Diameter Sh Interface Service facility
- **imsimgr**: SGSN IMSI Manager facility
- **imsue**: IMS User Equipment (IMSUE) facility
- **ip-arp**: IP Address Resolution Protocol facility
- **ip-interface**: IP interface facility
- **ip-route**: IP route facility
- **ipms**: Intelligent Packet Monitoring System (IPMS) logging facility
- **ipne**: IP Network Enabler (IPNE) facility
- **ipsec**: IP Security logging facility
- **ipsecdemux**: IPSec demux logging facility
- **ipsg**: IP Service Gateway interface logging facility
- **ipsgmgr**: IP Services Gateway facility
- **ipsp**: IP Pool Sharing Protocol logging facility
- **kvstore**: Key/Value Store (KVSTORE) Store facility
- **l2tp-control**: Layer 2 Tunneling Protocol (L2TP) control logging facility
- **l2tp-data**: L2TP data logging facility
- **l2tpdemux**: L2TP Demux Manager logging facility
- **l2tpmgr**: L2TP Manager logging facility
- **lagmgr**: Link Aggregation Group (LAG) manager logging facility
- **lcs**: Location Services (LCS) logging facility
- **ldap**: Lightweight Directory Access Protocol (LDAP) messages logging facility
- **li**: Refer to the *Lawful Intercept Configuration Guide* for a description of this command.
- **linkmgr**: SGSN/BSS SS7 Link Manager logging facility (2.5G only)
- **llc**: Logical Link Control (LLC) Protocol logging facility; for SGSN: logs the LLC layer between the GMM and the BSSGP layers for logical links between the MS and the SGSN
- **local-policy**: Local Policy Service facility
- **location-service**: Location Services facility
- **m3ua**: M3UA Protocol logging facility
- **magmgr**: Mobile Access Gateway manager logging facility
- **map**: Mobile Application Part (MAP) protocol logging facility
- **megadiammgr**: MegaDiameter Manager (SLF Service) logging facility
- **mme-app**: Mobility Management Entity (MME) Application logging facility

- **mme-misc**: MME miscellaneous logging facility
- **mmedemux**: MME Demux Manager logging facility
- **mmemgr**: MME Manager facility
- **mmgr**: Master Manager logging facility
- **mobile-ip**: Mobile IP processes
- **mobile-ip-data**: Mobile IP data facility
- **mobile-ipv6**: Mobile IPv6 logging facility
- **mpls**: Multiprotocol Label Switching (MPLS) protocol logging facility
- **mrme**: Multi Radio Mobility Entity (MRME) logging facility
- **mseg-app**: Mobile Services Edge Gateway (MSEG) application logging facility (This option is not supported in this release.)
- **mseg-gtpc**: MSEG GTP-C application logging facility (This option is not supported in this release.)
- **mseg-gtpu**: MSEG GTP-U application logging facility (This option is not supported in this release.)
- **msegmgr**: MSEG Demux Manager logging facility (This option is not supported in this release.)
- **mtp2**: Message Transfer Part 2 (MTP2) Service logging facility
- **mtp3**: Message Transfer Part 3 (MTP3) Protocol logging facility
- **multicast-proxy**: Multicast Proxy logging facility
- **nas**: Non-Access Stratum (NAS) protocol logging facility [MME 4G]
- **netwstrg**: Network Storage facility
- **npuctrl**: Network Processor Unit Control facility
- **npudrv**: Network Processor Unit Driver facility [ASR 5500 only]
- **npumgr**: Network Processor Unit Manager facility
- **npumgr-acl**: NPUMGR ACL logging facility
- **npumgr-drv**: NPUMGR DRV logging facility
- **npumgr-flow**: NPUMGR FLOW logging facility
- **npumgr-fwd**: NPUMGR FWD logging facility
- **npumgr-init**: NPUMGR INIT logging facility
- **npumgr-lc**: NPUMGR LC logging facility
- **npumgr-port**: NPUMGR PORT logging facility
- **npumgr-recovery**: NPUMGR RECOVERY logging facility
- **npumgr-rri**: NPUMGR RRI (Reverse Route Injection) logging facility
- **npumgr-vpn**: NPUMGR VPN logging facility
- **npusim**: NPUSIM logging facility [ASR 5500 only]

- **ntfy-intf**: Notification Interface logging facility [Release 12.0 and earlier versions only]
- **ocsp**: Online Certificate Status Protocol logging facility.
- **orbs**: Object Request Broker System logging facility
- **ospf**: OSPF protocol logging facility
- **ospfv3**: OSPFv3 protocol logging facility
- **p2p**: Peer-to-Peer Detection logging facility
- **pagingmgr**: PAGINGMGR logging facility
- **pccmgr**: Intelligent Policy Control Function (IPCF) Policy Charging and Control (PCC) Manager library
- **pdg**: Packet Data Gateway (PDG) logging facility
- **pdgdmgr**: PDG Demux Manager logging facility
- **pdif**: Packet Data Interworking Function (PDIF) logging facility
- **pgw**: Packet Data Network Gateway (PGW) logging facility
- **pmm-app**: Packet Mobility Management (PMM) application logging facility
- **ppp**: Point-To-Point Protocol (PPP) link and packet facilities
- **pppoe**: PPP over Ethernet logging facility
- **proclet-map-frwk**: Proclet mapping framework logging facility
- **push**: VPNMGR CDR push logging facility
- **radius-acct**: RADIUS accounting logging facility
- **radius-auth**: RADIUS authentication logging facility
- **radius-coa**: RADIUS change of authorization and radius disconnect
- **ranap**: Radio Access Network Application Part (RANAP) Protocol facility logging info flow between SGSN and RNS (3G)
- **rct**: Recovery Control Task logging facility
- **rdt**: Redirect Task logging facility
- **resmgr**: Resource Manager logging facility
- **rf-diameter**: Diameter Rf interface messages facility
- **rip**: Routing Information Protocol (RIP) logging facility [RIP is not supported at this time.]
- **rlf**: Rate Limiting Function (RLF) logging facility
- **rohc**: Robust Header Compression (RoHC) facility
- **rsvp**: Reservation Protocol logging facility
- **rua**: RANAP User Adaptation (RUA) [3G Femto GW - RUA messages] logging facility
- **s102**: S102 protocol logging facility

- **s102mgr**: S102Mgr logging facility
- **s1ap**: S1 Application Protocol (S1AP) Protocol logging facility
- **sabp**: Service Area Broadcast Protocol (SABP) logging facility
- **saegw**: System Architecture Evolution (SAE) Gateway facility
- **sbc**: SBc protocol logging facility
- **sccp:** Signalling Connection Control Part (SCCP) Protocol logging (connection-oriented messages between RANAP and TCAP layers).
- **sct**: Shared Configuration Task logging facility
- **sctp**: Stream Control Transmission Protocol (SCTP) Protocol logging facility
- **sef_ecs**: Severely Errored Frames (SEF) APIs printing facility
- **sess-gr**: SM GR facility
- **sessctrl**: Session Controller logging facility
- **sessmgr**: Session Manager logging facility
- **sesstrc**: session trace logging facility
- **sft**: Switch Fabric Task logging facility
- **sgs**: SGs interface protocol logging facility
- **sgsn-app**: SGSN-APP logging various SGSN "glue" interfaces (for example, between PMM, MAP, GPRS-FSM, SMS).
- **sgsn-failures**: SGSN call failures (attach/activate rejects) logging facility (2.5G)
- **sgsn-gtpc**: SGSN GTP-C Protocol logging control messages between the SGSN and the GGSN
- **sgsn-gtpu**: SGSN GTP-U Protocol logging user data messages between the SGSN and GGSN
- **sgsn-mbms-bearer**: SGSN Multimedia Broadcast/Multicast Service (MBMS) Bearer app (SMGR) logging facility
- **sgsn-misc**: Used by stack manager to log binding and removing between layers
- **sgsn-system**: SGSN System Components logging facility (used infrequently)
- **sgsn-test**: SGSN Tests logging facility; used infrequently
- **sgtpcmgr**: SGSN GTP-C Manager logging information exchange through SGTPC and the GGSN
- **sgw**: Serving Gateway facility
- **sh-diameter**: Sh Diameter messages facility
- **sitmain**: System Initialization Task main logging facility
- **sls**: Service Level Specification (SLS) protocol logging facility
- **sm-app**: SM Protocol logging facility
- **sms**: Short Message Service (SMS) logging messages between the MS and the SMSC

- **sndcp**: Sub Network Dependent Convergence Protocol (SNDCP) logging facility
- **snmp**: SNMP logging facility
- **sprmgr**: IPCF Subscriber Policy Register (SPR) manager logging facility
- **srdb**: Static Rating Database
- **srp**: Service Redundancy Protocol (SRP) logging facility
- **sscfnni**: Service-Specific Coordination Function for Signaling at the Network Node Interface (SSCF-NNI) logging facility
- **sscop**: Service-Specific Connection-Oriented Protocol (SSCOP) logging facility
- **ssh-ipsec**: Secure Shell (SSH) IP Security logging facility
- **ssl**: Secure Socket Layer (SSL) message logging facility
- **stat**: Statistics logging facility

Important The keyword **bulkstat** was added in StarOS release 21.1 to provide consistency with other CLI commands. Both keywords are supported for statistics logging facility.

- **supserv**: Supplementary Services logging facility [H.323]
- **system**: System logging facility
- **tacacsplus**: TACACS+ Protocol logging facility
- **tcap**: TCAP Protocol logging facility
- **testctrl**: Test Controller logging facility
- **testmgr**: Test Manager logging facility
- **threshold**: threshold logging facility
- **ttg**: Tunnel Termination Gateway (TTG) logging facility
- **tucl**: TCP/UDP Convergence Layer (TUCL) logging facility
- **udr**: User Data Record (UDR) facility (used with the Charging Service)
- **user-data**: User data logging facility
- **user-l3tunnel**: User Layer 3 tunnel logging facility
- **usertcp-stack**: User TCP Stack
- **vim**: Voice Instant Messaging (VIM) logging facility
- **vinfo**: VINFO logging facility
- **vmgctrl**: Virtual Media Gateway (VMG) controller facility
- **vmgctrl**: VMG Content Manager facility
- **vpn**: Virtual Private Network logging facility

- **wimax-data**: WiMAX DATA
- **wimax-r6**: WiMAX R6
- **wsg**: Wireless Security Gateway (ASR 9000 Security Gateway)
- **x2gw-app**: X2GW (X2 proxy Gateway, eNodeB) application logging facility
- **x2gw-demux**: X2GW demux task logging facility

level *severity_level*

level *severity_level*: Specifies the level of information to be logged from the following list which is ordered from highest to lowest:

- **critical** - display critical events
- **error** - display error events and all events with a higher severity level
- **warning** - display warning events and all events with a higher severity level
- **unusual** - display unusual events and all events with a higher severity level
- **info** - display info events and all events with a higher severity level
- **trace** - display trace events and all events with a higher severity level
- **debug** - display all events

pdu-data *pdu_format*

Specifies output format for the display of packet data units as one of:

- **none** - output is in raw format (unformatted).
- **hex** - output being displayed in hexadecimal format.
- **hex-ascii** - output being displayed in hexadecimal and ASCII similar to a main-frame dump.

pdu-verbosity *pdu_verboseness*

Specifies the level of verboseness to use in displaying of packet data units as an integer from 1 through 5, where 5 is the most detailed.

proclet *facility*

Shows the logs from a specific proclet facility. The available facilities are the same as those listed earlier.

since *from_date_time* [until *to_date_time*]

Default: no limit.

since *from_date_time*: indicates only the log information which has been collected more recently than *from_date_time* is to be displayed.

until *to_date_time*: indicates no log information more recent than *to_date_time* is to be displayed. **until** defaults to current time when omitted.

from_date_time and *to_date_time* must be formatted as YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss. Where:

- YYYY = 4-digit year
- MM = 2-digit month in the range 01 through 12
- DD = 2-digit day in the range 01 through 31
- HH = 2-digit hour in the range 00 through 23
- mm = 2-digit minute in the range 00 through 59
- ss = 2-digit second in the range 00 through 59

to_date_time must be a time which is more recent than *from_date_time*.

The use of the **until** keyword allows for a time range of log information while only using the **since** keyword will display all information up to the current time.

| { 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 log files for general maintenance or troubleshooting system issues.

Example

The following command displays log information for the *a11mgr* facility starting with July 1th, 2011 at midnight.

```
show logs facility allmgr since 2011:07:11:00:00
```

The following command displays the log information for call ID *FE881D32* only in active logs.

```
show logs active callid FE881D32
```

show lte-policy

Displays information for Long term Evolution (LTE) policy configurations on this system including congestion action profiles, handover restriction lists, paging maps, paging profiles, subscriber maps, and tracking area identifiers (TAIs).

Product

HeNBGW

MME

SAEGW

S-GW

Privilege

Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
show lte-policy { cause-code-group { name group_name | summary } |
congestion-action-profile { name congest_profile_name | summary } |
foreign-plmn-guti-mgmt-db { name db_name | summary }  | henbgw { mme-pool
{ name  mme_pool_name | summary }  | qci-dscp-mapping-table { name table_name
 | summary } | overload-control | s1-reset | session-recovery }|
ho-restriction-list { name ho_list_name | summary } | lte-emergency-profile
 { name  emer_profile_name | summary }  | mme { henbgw mgmt-db { name
henbgw_mgmtdb_name  | summary } | paging cache parameters | paging-map { name
  page_map_name | summary } | paging-profile { name page_profile_name | summary
 } | peer-map { name sub_map_name | summary } | subscriber-map { name
sub_map_name | summary } | tai-list-db { name  tai_list_name summary } |
tai-mgmt-db { name tai_name [ tai-mgmt-obj name obj_name | tai-custom-list
tac cstm_tac_value ] | summary } } [ | { grep grep_options | more } ]
```

cause-code-group { name *group_name* | summary }

This MME-specific keyword displays information about the Cause Code Groups configured on this system.

name *group_name*: Displays information about a specific cause code group configured on this system. *group_name* must be an existing cause code group, expressed as an alphanumeric string of 1 to 16 characters.

summary: Displays summarized information about all cause code groups configured on this system.

congestion-action-profile { name *congest_profile_name* | summary }

Displays information about MME congesting action profiles configured on this system.

name *profile_name*: Displays information about a specific congestion action profile configured on this system. *profile_name* must be an existing HO restriction list, expressed as an alphanumeric string of 1 to 64 characters.

summary: Displays summarized information about all congestion action profiles configured on this system.

foreign-plmn-guti-mgmt-db { name *db_name* | summary }

This MME-specific keyword displays information about LTE Foreign PLMN GUTI management databases configured on this system.

name *db_name*: Displays information about a specific management database configured on this system. *db_name* must be an existing management database, expressed as an alphanumeric string of 1 to 64 characters.

summary: Displays summarized information about all Foreign PLMN GUTI management databases configured on this system.

henbgw { mme-pool { name *mme_pool_name* | summary } | qci-dscp-mapping-table { name *table_name* | summary } | overload-control | session-recovery }

This HeNBGW keyword displays information about HeNBGW configured on this 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.

mme-pool shows mme pool.

name *mme_pool_name*: Displays detailed information about specified MME Pool configured on this system. *mme_pool_name* must be an existing management database, expressed as an alphanumeric string of 1 to 63 characters.

summary: Displays summarized information about MME Pool configured on this system.

qci-dscp-mapping-table shows qci-dscp-mapping-table information.

name *table_name*: Displays information for specific qci-dscp-mapping-table.*table_name* must be qci-dscp-mapping-table expressed as an alphanumeric string of 1 to 63 characters.

summary: Displays summary of all qci-dscp-mapping-table.

overload-control: Displays information about overload control.

s1-reset: Displays information about s1 reset.

session-recovery: Displays information about session recovery.

ho-restriction-list { name *list_name* | summary }

Displays information about handover restriction lists configured on this system.

name *ho_list_name*: Displays information about a specific handover restriction list configured on this system. *name* must be an existing HO restriction list, expressed as an alphanumeric string of 1 to 64 characters.

summary: Displays summarized information about all handover restriction lists configured on this system.

lte-emergency-profile { name *emer_profile_name* | summary }

Displays information about LTE emergency profiles configured on this system.

name *emer_profile_name*: Displays information about a specific LTE emergency profile configured on this system. *emer_profile_name* must be an existing LTE emergency profile, expressed as an alphanumeric string of 1 to 64 characters.

summary: Displays summarized information about all LTE emergency profiles configured on this system.

mme paging cache parameters

Displays the configured MME paging cache timeout and MME paging cache size configured with the **mme paging cache** command in the LTE Policy configuration mode.

paging-map { name *page_map_name* | summary }

Displays information about LTE paging maps configured on this system.

name *page_map_name*: Displays information about an existing LTE paging map specified as an alphanumeric string of 1 through 64 characters.

summary: Displays summarized information about all LTE paging maps configured on this system.

paging-profile { name *page_profile_name* | summary }

Displays information about LTE paging profiles configured on this system.

name *page_profile_name*: Displays information about an existing LTE paging profile specified as an alphanumeric string of 1 through 64 characters.

summary: Displays summarized information about all LTE paging profiles configured on this system.

peer-map { name *name* | summary }

Displays information about peer maps configured on this system.

name *map_name*: Displays information about an existing peer map specified as an alphanumeric string of 1 through 64 characters.

summary: Displays summarized information about all peer maps configured on this system.

subscriber-map { name *name* | summary }

Displays information about subscriber maps configured on this system.

name *sub_map_name*: Displays information about an existing subscriber map specified as an alphanumeric string of 1 through 64 characters.

summary: Displays summarized information about all subscriber maps configured on this system.

tai-list-db { name *tai_list_ name* | summary }

Displays information about TAI list databases configured on this system

name*tai_list_ name*: Displays information about specified TAI list database as an alphanumeric string of 1 through 64 characters.

summary: Displays summarized information about specified TAI list databases configured on this system.

tai-mgmt-db { name *name* [tai-mgmt-obj name *obj_name* | tai-custom-list tac *cstm_tac_value*] | summary }

Displays information about TAI management databases configured on this system.

name *tai_name*: Displays information about an existing TAI management database specified as an alphanumeric string of 1 through 64 characters.

tai-mgmt-obj name *obj_name* : Filters the information by the specified TAI Management Object name, where *obj_name* is a string from 1 through 64 characters.

tai-custom-list tac *cstm_tac_value* : Filters the information by the specified Custom TAI List TAC, where *cstm_tac_value* is an integer from 0 through 65535.

summary: Displays summarized information about all TAI management databases configured 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 *CLI Overview* chapter.

Usage Guidelines

Use this command to display information for LTE policy configurations on this system including congestion action profiles, handover restriction lists, paging maps, paging profiles, subscriber maps, and tracking area identifiers (TAIs).

Example

The following command displays information about a subscriber map named *map3*:

```
show lte-policy subscriber-map name map3
```

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