Exec Mode show Commands (T-Z)

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 chapter includes the commands **show tacacs** through **show version**.

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 tacacs

Displays information about all active Terminal Access Controller Access-Control System Plus (TACACS+) sessions.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show tacacs [ client | priv-lvl | session { all | id` *`session_id`* **`| idle | statistics } | summary ] [ | { grep` *`grep_options`* **`| more } ]`**

show tacacs

This command provides the following TACACS+ information:

- Individual active session number with the following additional session-specific information:
  - login user name
  - login tty
  - time of login
  - login server priority
  - current session state
  - current privilege level
  - remote client application (if applicable)
  - remote client ip address (if applicable)
  - last server reply status
- Total number of TACACS+ sessions

[client | priv-lvl | session | summary]

Optional filters are available for the output of the **show tacacs** command:

- **client** – Display information about the TACACS+ client.
- **priv-lvl** – Display TACACS+ priv-level authorization attributes for StarOS administrative levels. Only supported in StarOS Release 17.3 and higher.
- **session** – Display information about the TACACS+ sessions.
  - **all** – Displays all TACACS+ sessions with session id, idle threshold, idle time, and application type.
  - **id** *session_id* – Session ID to be displayed. *session_id* must be an integer from 1 to 128.
  - **idle** – Lists all idle TACACS+ sessions in the order of most idle sessions.
  - **statistics** – Display statistics about the TACACS+ sessions.
- **summary** – Display summary information about the TACACS+ sessions.

| { grep *grep_options* | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output 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 detailed session information for all active TACACS+ sessions.

Important This command is available on version 11.0 and later systems.

Example

```
show tacacs
```

show task

Displays information about system tasks.

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 task { info | memory | resources | table } [card** *card_num* **] [facility** *facility* **{ all | instance** *id* **}] [process** *process_name* **all] [max] [| { grep** *grep_options* **| more }]**

{ info | memory | resources | table }

Specifies the type of information to be displayed and scope of tasks to include in output.

info: Displays detailed task information.

memory: Displays detailed task memory usage information.

resources: Displays resource allocation and usage information for all tasks.

table: Displays identification information in tabular format for all tasks.

Note In Release 21.1, the Active Health Monitor (AHM) functionality is added to the Resource Manager (RMMGR) to aid in the monitoring of specific processes and proactively collect required debug information at runtime without manual intervention.

When a process enters the "warn" or "over" state for a memory limit, CPU limit, or both, the RMMGR triggers a logging mechanism that proactively collects the memory heap/CPU profiler information, writes it into a file and stores it locally.

The files that are stored locally on the CPU of each individual processing card are then transferred to HD-RAID in the preconfigured directory location.

card *card_num*

Default: all powered on cards.

Specifies a single card for which task information is to be displayed where *card_num* must be an integer from 1 to 48 for the ASR 5000 and 1 to 20 for the ASR 5500.

facility *facility* { all | instance *id* max }

Default: all facilities.

Specifies the list of facilities for which task information may be displayed. A specific instance of the facility may be displayed as specified by ID or all instances may be displayed. The value of *id* must be an integer from 0 to 10000000. *facility* must be one of:

- **a11mgr**: A11 Interface Manager facility
- **aaamgr**: AAA Manager Facility
- **aaaproxy**: AAA Proxy manager Facility
- **acsctrl**: Active Charging Service (ACS) Controller Facility [Release 11.0 and earlier versions only]
- **acsmgr**: Active Charging Service (ACS) Manager Facility
- **afctrl**: Fabric Manager [ASR 5500 only]
- **afmgr**: Fabric Manager [ASR 5500 only]
- **alcapmgr**: ALCAP Manager
- **asngwmgr**: ASN Gateway Manager
- **asnpcrmgr**: ASN Paging/Location-Registry (ASN-PC) Manager
- **bfd**: Bidirectional Forwarding Detection
- **bgp**: Border Gateway Protocol (BGP) Facility
- **bngmgr**: BNG Manager
- **bulkstat**: Bulk Statistics Manager Facility
- **callhome**: Call Home Controller
- **cdrmod**: Charging Detail Record Module

- **cli**: Command Line Interface Facility
- **connproxy**: Proxy for connections from same card or chassis
- **cspctrl**: Card Slot Port controller Facility
- **cssctrl**: Content Service Steering Controller
- **dcardctrl**: IPSec Daughter-card Controller Logging Facility
- **dcardmgr**: IPSec Daughter-card Manager Logging Facility
- **dgmbmgr**: Diameter Gmb Application Manager
- **dhmgr**: Distributed Host Manager
- **diamproxy**: Diameter Proxy
- **drvctrl**: Driver Controller Facility
- **egtpegmgr**: EGTP Egress Demux Manager
- **egtpinmgr**: EGTP Ingress Demux Manager
- **evlogd**: Event Log Daemon Facility
- **famgr**: Foreign Agent Manager Facility
- **gtpcmgr**: GTP-C Protocol Logging facility (GGSN product only)
- **gtpumgr**: GTP-U Demux Manager
- **h248prt**: H.248 Protocol Task [Release 11.0 and earlier versions only]
- **hamgr**: Home Agent Manager Facility
- **hatcpu**: High Availability Task CPU Facility
- **hatsystem**: High Availability Task Facility
- **hdctrl**: HD Controller
- **henbgwdemux**: Home eNodeB Gateway demux manager

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**: Home eNodeB Gateway Manager

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.

- **hnbmgr**: HNBGW HNB Manager

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.

- **hwctrl**: Hardware Monitor Controller
- **hwmgr**: Hardware Monitor Manager
- **imsimgr**: SGSN IMSI Manager
- **ipsecctrl**: IP Security Controller Facility
- **ipsecmgr**: IP Security Manager Facility
- **ipsgmgr**: IP Services Gateway Facility
- **kvctrl**: KV Controller
- **kvmgr**: KV Manager
- **l2tpdemux**: L2TP Demultiplexor (LNS) Facility
- **l2tpmgr**: L2TP Manager Facility
- **lagmgr**: Link Aggregation Group (LAG) Manager
- **linkmgr**: SGSN/SS7 Link Manager
- **magmgr**: Mobile Access Gateway Manager
- **megadiammgr**: MegaDiameter Manager
- **mmedemux**: MME Demux Manager logging facility
- **mmemgr**: MME Manager logging facility
- **mmgr**: SGSN/SS7 Master Manager
- **mpls_sig**: Multiprotocol Label Switching
- **mptest**: Migration Performance Test on Packet Accelerator Card
- **netwstrg**: Network Storage Manager [Release 11.0 and earlier versions only]
- **npuctrl**: Network Processor Unit Control Facility
- **npudrv**: Network Processor Unit Driver Facility [ASR 5500 only]
- **npumgr**: Network Processor Unit Manager Facility
- **npusim**: Network Processor Unit Simulator [ASR 5500 only]
- **nputst**: Network Processor Unit Tester
- **nsctrl**: Charging Service Controller [Release 11.0 and earlier versions only]
- **nsmgr**: Charging Service Process Manager [Release 11.0 and earlier versions only]
- **orbns**: Object Request Broker Notification Server Facility

- **orbs**: Object Request Broker System Facility
- **ospf**: Open Shortest Path First Facility
- **ospfv3**: Open Shortest Path First (OSPFv3)
- **pdgmgr**: PDG Manager
- **phsgwmgr**: PHS Gateway manager
- **phspcmgr**: PHS Paging Controller manager
- **rct**: Recovery Control Task Facility
- **rdt**: Redirect Task Facility
- **rip**: Routing Information Protocol Facility
- **rmctrl**: Resource Manager Controller Facility
- **rmmgr**: Resource Manager Facility
- **sct**: Shared Configuration Task Facility
- **sessctrl**: Session Controller Facility
- **sessmgr**: Session Manager Facility
- **sesstrc**: Session Trace Collection task
- **sft**: Switch Fabric Monitoring Task
- **sgtpcmgr**: SGSN GTPC Manager
- **sipcdprt**: SIP Call Distributor Task [Release 11.0 and earlier versions only]
- **sitmain**: System Initialization Task Main Facility
- **sitparent**: Card based system initialization facility that applies to the MIO card.
- **snmp**: SNMP Protocol Facility
- **srdb**: Static Rating Database
- **testctrl**: Test Controller
- **testmgr**: Test Manager
- **threshold**: Threshold Server Facility
- **vpnctrl**: Virtual Private Network Controller Facility
- **vpnmgr**: VPN Manager Facility
- **zebos**: ZEBOS™ OSPF Message Facility

all: Displays information for all instances of the specified facility.

instance *id*: Displays information for the facility instance that is specified as an integer from 0 to 10000000.

process *process_name* all

Display information for all instances of the specified process. must be one of the following process names:

- **ftpd**: File Transfer Protocol Daemon
- **inetd**: Internet Superserver Daemon
- **nsproc**: NetSpira Packet Processor
- **ntpd**: Network Time Protocol Daemon
- **orbnsd**: Object Request Broker Notification Server
- **ping**: Ping
- **pvmd-wrapper**: NetSpira Messenger Daemon
- **pvmgs**: NetSpira Messenger Daemon
- **rlogin**: Remote Login
- **sftp-server**: Secure File Transfer Protocol Server
- **sitreap**: System Initialization Task Cleanup Process
- **sn_resolve**: DNS Resolver Process
- **ssh**: Secure Shell
- **sshd**: Secure Shell Daemon
- **telnet**: Telnet
- **telnetd**: Telnet daemon
- **tftpd**: Trivial File Transfer Protocol Daemon
- **traceroute**: Traceroute

max

Default: current usage levels are displayed.

Displays the maximum usage levels for tasks as opposed to the current usage levels.

max is valid only along with the **resources** keyword.

| { grep *grep_options* | more }

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

Displays task information as part of a system troubleshooting for unexpected behavior.

Important This command is not supported on all platforms.

Note The following conditions may cause Shared Configuration Task (SCT) CPU spikes:

- Frequent CLI session initiation that includes both failed and successful session may cause SCT CPU spike.

  It is therefore recommended to use an alternate to CLI, such as bulkstats if there is a requirement to view the statistics. Also, avoid exiting CLI sessions and using scripts that initiate CLI sessions.

- "show" commands like "show configuration".

  It is recommended to use the monitoring commands sparingly and only on need-basis.

- Configuration monitoring can drive high CPU usage and also spike the SCT CPU. Note that higher the configuration, higher the CPU usage.

  It is recommended to monitor the configuration only when required.

- SDR configuration and periodicity. Periodic data collection adds load to the SCT and to the entire CPU. Therefore, ensure that the SDR is optimally configured. Use the CLI "show configuration collection definition" to check which CLI collections are enabled, review the configuration, and configure only required items.

Example

The following commands provide some examples of the combinations of options that may be used to display task information.

```
show task info facility hatspc all
show task info facility hatspc instance 456
show task resources facility zebos all
show task table facility ospf
show task table card 8 facility cli all
show task table card 5 facility cli all
show task resources facility rip all max
```

show tcap statistics

This command displays the collected traffic statistics that have passed through the SS7 Transaction Capabilities Application Part (TCAP) layer.

Product SGSN

Privilege Security Administrator, Administrator, Operator

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show tcap statistics [camel-service [all | name *camel_srvc* **] | map-service [all | name** *map_srvc* **]] [| { grep** *grep_options* **| more }]**

camel-service [all | name *camel_srvc*]

Displays TCAP statistics for either all Customized Applications for Mobile networks Enhanced Logic (CAMEL) services or only for the named CAMEL service.

map-service [all | name *mapl_srvc*]

Displays TCAP statistics for either all Mobile Application Part (MAP) services or only for the named MAP service.

| { grep *grep_options* | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output 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 display the collected TCAP statistics for MAP or CAMEL services.

Example

The following command displays the collected statistics for a MAP service named *MAP-Tewk*.

```
show tcap statistics map-service name MAP-Tewk
```

show temperature

Displays the current temperature on all installed cards. Also displays the temperature of upper and lower fan trays. Temperature readings are acquired from sensors located on theses components.

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 temperature [verbose] [| { grep *grep_options* **| more }]**

| { grep *grep_options* | more }

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

verbose

Indicates that the output is to contain detailed information.

Usage Guidelines Verify current temperature of components in chassis.

Example

```
show temperature
show tempterature verbose
```

show terminal

Displays the current terminal settings for number of lines in length and number of characters in width.

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 terminal [| { grep** *grep_options* **| more }]**

| { grep *grep_options* | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output 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 verify current terminal settings in case the output displayed appears to have line breaks/wraps in unexpected places.

Example

```
show terminal
```

show threshold

Displays thresholding information for 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 threshold [ default ]`

`[ default ]`

Used to display the system's thresholding default values.

Usage Guidelines

Use this command to display information on threshold value configuration and activity.

Example

The following command displays configuration information pertaining to threshold values configured on the system:

`show threshold`

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

show transaction-rate

Displays transaction-rate (per sec) for given services.

Product

ePDG

PGW

SAE-GW

Privilege

Security Administrator, Administrator, Inspector, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

show transaction-rate { epdg-service | pgw-service | saegw-service [all | name *srvc_name* **] } [| { grep** *grep_options* **| more }]**

epdg-service

Displays transaction-rate (per sec) for all or given epdg services.

pgw-service

Displays transaction-rate (per sec) for all or given pgw services.

saegw-service

Displays transaction-rate (per sec) for all or given SAE-GW services.

all

Displays consolidated transaction-rate (per sec) for all epdg / pgw services configured on this system.

name *srvc_name*

Displays node level transaction-rate (per sec) for given epdg / pgw service as an alphanumeric string of 1 through 63 characters.

[| { grep *grep_options* | more }]

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

Syntax Description

Use this command to display the transaction-rate (per sec) for given services configured on this system.

Example

The following command displays the transaction-rate (per sec) for given epdg service by name *epserv1* configured on this system:

transaction-rate epdg-service name epserv1

show url-blacklisting database

Displays URL Blacklisting static database configurations.

Product

CF

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

show url-blacklisting database [all | url *url* **| facility acsmgr { all | instance** *instance* **}] [| { grep** *grep_options* **| more }]**

all

Displays configurations of all URL Blacklisting databases present in the default or override directory.

facility acsmgr { all | instance *instance* }

Displays configurations of URL Blacklisting database configuration per facility/ACSMgr instance.

all: Displays URL Blacklisting database configuration of all ACSMgrs.

instance *instance*: Displays URL Blacklisting database configuration for the instance number of the database specified as an integer from 1 through 10000000.

url *url*

Displays configurations of the URL Blacklisting database specified in the database's URL expressed as an alphanumeric string of 1 through 512 characters.

| { grep *grep_options* | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output 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 configurations associated with in-memory and on-flash Blacklisting database. The **show url-blacklisting database** command displays the active database that is loaded, and is the one set by either the default or override CLI commands.

Example

The following command displays configurations of all the databases present in default or override directory, indicating one as Active and rest as Not Loaded:

```
show url-blacklisting database all
```

The following command displays configurations of the */flash/bl/optblk.bin* database:

```
show url-blacklisting database url /flash/bl/optblk.bin
```

The following command displays database configuration for the ACSMgr instance *1*:

```
show url-blacklisting database facility acsmgr instance 1
```

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

show user-plane-service

Displays user plane service information for the system.

Product

UPF

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

Syntax

```
show user-plane-service  [ service_name ] { local-addresses | statistics
 [all | id ] }
```

[service_name]

Specifies the name of the configured user plane service. It includes following user plane services:

- aaa-group
- accounting-policy
- all
- appliance-group
- bandwidth-policy
- charging-action
- content-filtering
- edns
- edr-format
- firewall
- flow-control-counters
- fw-and-nat
- group-of-prefixed-urls
- group-of-ruledefs
- gtpp-group
- gtpu
- hostpool
- imsi-pool

- inline-services
- ip-access-list
- monitoring-key-urr-id-list
- name
- nrf
- pdn-instance
- portmap
- qos-group-of-ruledefs
- readdress-server-list
- regex
- rulebase
- ruledef
- service-chain
- service-scheme
- session-priority-profile
- sessions
- statistics
- subscriber-base
- subscriber-class
- timedef
- traffic-optimization
- traffic-steering
- trigger-action
- trigger-condition
- url-blockedlisting
- url-sni-pool
- xheader-format

local-addresses

Lists the local gtpu addresses and the current number of active sessions associated with each address.

statistics

Displays the Node level GTPU statistics.

Example

Following show CLI displays the number of active bearers/sessions using specific bind address.

show user-plane-service gtpu local-addresses

The following show command displays the statistics per GTPU bind address.

show user-plane-service gtpu statistics local-address

Usage Guidelines Use this command to display information about packet drops and their respective causes, which are pegged at instance and session levels.

show version

Displays the version information for the current system image or for a remote image.

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 version [** *url* **] [all | verbose] [| { grep** *grep_options* **| more }]**

url

Specifies the location of a configuration file for which to display version information. The *url* may refer to a local or a remote file and must be entered in the following format:

For the ASR 5000:

[file:] { /flash | /pcmcia1 | /hd } [/*directory* **] /***file_name*
tftp:// { *host* **[** *:port#* **] } [/***directory* **] /***file_name*
[http: | ftp: | sftp:] // [*username* **[** *:password* **] @] {** *host* **} [** *:port#* **] [/***directory* **] /***file_name*

For the ASR 5500:

[file:] { /flash | /usb1 | /hd } [/*directory* **] /***file_name*
tftp:// { *host* **[** *:port#* **] } [/***directory* **] /***file_name*
[http: | ftp: | sftp:] // [*username* **[** *:password* **] @] {** *host* **} [** *:port#* **] [/***directory* **] /***file_name*

For VPC:

[file:] { /flash | /usb1 | /usb2 /cdrom1 } [/*directory* **] /***file_name*
tftp:// { *host* **[** *:port#* **] } [/***directory* **] /***file_name*
[http: | ftp: | sftp:] // [*username* **[** *:password* **] @] {** *host* **} [** *:port#* **] [/***directory* **] /***file_name*

Important Do not use the following characters when entering a string for the field names below: "/" (forward slash), ":" (colon) or "@" (at sign).

directory is the directory name.

filename is the actual file of interest.

username is the user to be authenticated.

password is the password to use for authentication.

host is the IP address or host name of the server.

port# is the logical port number that the communication protocol is to use.

all | verbose

all: displays all image information.

verbose: displays detailed information.

The **verbose** keyword may not be used in conjunction with a URL specification.

| { grep *grep_options* | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output 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 Display the version information to verify the image versions loaded in preparation for maintenance, upgrades, etc.

You can display additional release build information by running the Exec mode **show build** command.

Example

The following commands display the version information with the basic level of output and the detailed level, respectively.

```
show version
show version verbose
```

show wsg-application

Displays wsg-application information.

Product SecGW (WSG)

Privilege Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show wsg-application ( all | name |` *`application_name`* **`[ counter ] [ | { grep`** *`grep_options`* **`| more } ] | statistics [ all ] [ name ] [ | { grep`** *`grep options`* **`| more } ] }`**

all

Displays information for all configured application

name *application_name*

Displays specific application. Must be followed by application name which is a string of size 1 through 63.

counter

Displays information for all configured application.

statistics

Displays information for all configured application.

[| { grep *grep options* | more }] }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output 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 display wsg-application information.

Example

The following example displays information for all configured application:

```
show wsg-application statistics
```

show wsg-lookup

Displays the current priority settings of subnet components for site-to-site tunnels in WSG services.

Product

SecGW (WSG)

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description **show wsg-lookup**

Usage Guidelines Use this command to display current WSG lookup priority settings,

Examples

show wsg-lookup

show wsg-service

Displays information about WSG service calls and configured services.

Product SecGW (WSG)

Privilege Security Administrator, Administrator, Operator

Command Modes Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description **show wsg-service (all | name |** *srvc_name* **| statistics [name** *srvc_name* **| peer-address** *ip_address* **] [| { grep** *grep_options* **| more }]**

all

Displays information for all configured services.

name *srvc_name*

Displays information for the specified service name.

| statistics [name *srvc_name* | peer-address *ip_address*

Displays information collected for the WSG service since the last VPC-VSM reload or clear command

You can display information for all WSG services (default), for named service or for a specific peer IP address. The peer *ip_address* can be specified in IPv4 dotted decimal or IPv5 colon-separated hexadecimal notation.

| { grep *grep_options* | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output 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 This command displays information about all or a specified WSG service.

Example

The following command displays information about all WSG services:

```
show wsg-service all
```

show x2gw-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 is used to display the X2GW service related information.

Product

HeNBGW

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show x2gw-service { all | enb-association [ all ] | statistics [ sctp | x2ap ] }[ | { grep grep_options | more } ]`

all

Displays all the X2GW services.

enb-association

Displays the information about (H)ENB associations.

statistics

Displays the X2GW service statistics.

| { grep *grep_options* | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output 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 display the X2GW service related information.

Example

The following command displays the X2GW service statistics.

```
show x2gw-service statistics
```