Exec Mode Commands (D-S)

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

Command Modes

This chapter contains the commands in the Exec Mode from **debug** to **system**.

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).

debug bfd

Enables or disables the debug options for Bidirectional Forwarding Detection BFD) debugging. If logging is enabled, results are sent to the logging system.

Product

All

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`[ no ] debug bfd { all | events ipc-error | ipc-events | nsm | packet | session }`

no

Indicates the IP debugging is to be disabled for the IP interfaces/function specified.

bfd | interface *name* | route

Specifies which IP interfaces/function to debug.

all: enables debug for all BFD items.

events: enables debug for BFD events.

ipc-error: enables debug for BFD Inter-process communication (IPC) errors.

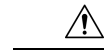
ipc-events: enables debug for BFD Inter-process communication (IPC) events.

nsm: enables debug for BFD Network Service Manager messages.

packet: enables debug for BFD packets.

session: enables debug for BFD sessions.

Usage Guidelines The debug bfd command is valuable when troubleshooting network problems with BFD-enabled BGP routers. The debugging is stopped by using the **no** keyword.



Caution Issuing this command could negatively impact system performance depending on system configuration and/or loading.

Example

The following commands enable/disable debugging for BFD.

```
debug bfd
no debug bfd
```

debug ip

Enables or disables the debug options for IP debugging. If logging is enabled, results are sent to the logging system.

Product All

Privilege Security Administrator, Administrator, Operator

Command Modes Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description **`[ no ] debug ip { arp | interface | route }`**

no

Indicates the IP debugging is to be disabled for the IP interfaces/function specified.

arp | interface *name* | route

Specifies which IP interfaces/function to debug.

arp: indicates debug is to be enabled for the address resolution protocol.

interface: indicates debug is to be enabled for the IP interfaces.

route: indicates debug is to be enabled for the route selection and updates.

Usage Guidelines The debug IP command is valuable when troubleshooting network problems between nodes. The debugging is stopped by using the **no** keyword.

Caution Issuing this command could negatively impact system performance depending on system configuration and/or loading.

Example

The following commands enable/disable debugging for ARP.

```
debug ip arp
no debug ip arp
```

The following enables/disables debugging for IP interfaces.

```
debug ip interface
no debug ip interface
```

The following enables/disables debugging for routing.

```
debug ip route
```

```
no debug ip route
```

debug ip bgp

Enables or disables BGP (Border Gateway Protocol) debug flags. If logging is enabled, results are sent to the logging system.

Product HA

Privilege Security Administrator, Administrator, Operator

Command Modes Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

```
[ no ] debug ip bgp { all | event | filters | fsm | keepalives | updates
 { inbound | outbound } }
```

no

Disables the specified BGP debug flags.

all

Enables all BGP debug flags.

event

Enables debugging of all BGP protocol events.

filters

Enables debugging of all BGP filters.

fsm

Enables debugging of BGP Finite State Machine

keepalives

Enables debugging of all BGP keepalives.

updates {inbound | outbound}

Enables debugging of BGP updates.

inbound: Debug all BGP inbound updates.

outbound: Debug all BGP outbound updates.

Usage Guidelines

Use this command to enable or disable BGP debug flags.

Example

The following command disables all BGP debug flags enabled by any of the **debug ip bgp** commands:

```
no debug ip bgp all
```

The following command enables all BGP debug flags:

```
debug ip bgp all
```

debug ip ospf all

Enables or disables all OSPF (Open Shortest Path First) debug flags. If logging is enabled, results are sent to the logging system.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
[ no ] debug ip ospf all
```

no

Disable all OSPF debug flags.

Usage Guidelines

Use this command to enable or disable all OSPF debug flags.

Example

The following command disables all OPSF debug flags enabled by any of the **debug ip ospf** commands:

```
no debug ip ospf all
```

The following command enables all OSPF debug flags:

```
debug ip ospf all
```

debug ip ospf event

Enables or disables debugging of OSPF protocol events. If logging is enabled, results are sent to the logging system. If no keywords are specified, all events are enabled for debugging.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

```
[ no ] debug ip ospf event [ abr | asbr | vl | lsa | os | router ]
```

no

Disables debugging the specified OSPF event. If no keywords are specified, all events are disabled.

abr

Enables debugging of Area Border Router (ABR) events.

asbr

Enables debugging of Autonomous System Boundary Router (ASBR) events.

vl

Enables debugging of Virtual Link (VL) events.

lsa

Enables debugging of link state advertisement (LSA) events.

os

Enables debugging of operating system (OS) events.

router

Enables debugging of router events.

Usage Guidelines

Use this command to output debug information for OSPF events.

Example

To enable all event debug information, enter the following command;

```
debug ip ospf event
```

To disable all event debug information, enter the following command;

```
no debug ip ospf event
```

debug ip ospf ism

Enables or disables OSPF Interface State Machine (ISM) troubleshooting, based on ISM information type. If no keywords are specified all ISM information types are enabled. If logging is enabled, results are sent to the logging system.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

```
[ no ] debug ip ospf ism [ events | status | timers ]
```

no

Disables debugging the specified ISM information. If no keywords are specified, all information is disabled.

events

Enables debugging ISM event information.

status

Enables debugging ISM status information.

timers

Enables debugging ISM timer information.

Usage Guidelines

Use this command to output ISM debug information.

Example

To enable all ISM debug information, enter the following command;

```
debug ip ospf ism
```

To disable all ISM debug information, enter the following command;

```
no debug ip ospf ism
```

debug ip ospf lsa

Enables or disables troubleshooting on OSPF Link State Advertisements (LSAs), based on the specific LSA option. If no keywords are specified, all options are enabled. If logging is enabled, results are sent to the logging system.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
[ no ] debug ip ospf lsa [ flooding | generate | install | refresh |
maxage | refresh ]
```

no

Disables the specified LSA debug information. If no keyword is specified, all LSA debug information is disabled.

flooding

Enables LSA flooding information.

generate

Enables LSA generation information.

install

Enables LSA install information.

maxage

Enables LSA maximum age information in seconds. The maximum age is 3600 seconds.

refresh

Enables LSA refresh information.

Usage Guidelines

Use this command to output debug information for LSAs.

Example

To enable all LSA debug information, enter the following command;

```
debug ip ospf lsa
```

To disable all LSA debug information, enter the following command;

```
no debug ip ospf lsa
```

debug ip ospf nsm

Enables or disables troubleshooting OSPF Neighbor State Machines (NSMs), based on the specific NSM information type. If no keyword is specified, all NSM information types are enabled. If logging is enabled, results are sent to the logging system.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
[ no ] debug ip ospf nsm [ status | events | timers ]
```

no

Disables the debugging the specified NSM information type. If no keyword is specified, all information types are disabled.

events

Enables debugging NSM event information.

status

Enables debugging NSM status information.

timers

Enables debugging NSM timer information.

Usage Guidelines

Use this command to output debug information for OSPF NSMs

Example

To enable all NSM debug information, enter the following command;

```
debug ip ospf nsm
```

To disable all NSM debug information, enter the following command;

```
no debug ip ospf nsm
```

debug ip ospf packet

Enables or disables troubleshooting of specific OSPF packet information. If logging is enabled, results are sent to the logging system.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
[ no ] debug ip ospf packet { all | dd | hello | ls-ack | ls-request |
ls-update } [ send | recv ] [ detail ]
```

no

Disable debugging of the specified packet information.

all

Enables debugging all OSPF packet information.

dd

Enables debugging database descriptions.

hello

Enables debugging hello packets.

ls-ack

Enables debugging link state acknowledgements.

ls-request

Enables debugging link state requests.

ls-update

Enables debugging link state updates.

send

Enables debugging only on sent packets.

recv

Enables debugging only on received packets.

detail

Enables detailed information in the debug output.

Usage Guidelines

Use this command to output specific OSPF packet information.

Example

To enable all packet debug information, enter the following command;

```
debug ip ospf packet all
```

To disable all route debug information, enter the following command;

```
no debug ip ospf packet all
```

debug ip ospf route

Sets the route calculation method to use in debugging OSPF routes. If no route calculation method is specified, all methods are enabled. If logging is enabled, results are sent to the logging system.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`[ no ] debug ip ospf route [ ase | ia | install | spf ]`

no

Disables debugging of route information. If no keyword is specified all information types are disabled.

ase

Enables debugging information on autonomous system external (ASE) route calculations.

ia

Enables debugging information on Inter-Area route calculations.

install

Enables debugging information on route installation.

spf

Enables debugging information on Shortest Path First (SPF) route calculations.

Usage Guidelines

Use this command to output debug information for OSPF routes.

Example

To enable all route debug information, enter the following command;

`debug ip ospf route`

To disable all route debug information, enter the following command;

`no debug ip ospf route`

debug ip ospf router

Sets the debug option for OSPF router information. If no keyword is specified, all router information is enabled. If logging is enabled, results are sent to the logging system.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`[ no ] debug ip ospf router [ interface | redistribute ]`

no

Disables the specified router debug information. If no keyword is specified, all router information is disabled.

interface

Enables router interface information.

redistribute

Enables router redistribute information.

Usage Guidelines

Use this command to output debug information for the OSPF router.

Example

To enable all router debug information, enter the following command;

`debug ip ospf router`

To disable all router debug information, enter the following command;

`no debug ip ospf router`

debug ipv6 ospf all

Enables or disables all OSPFv3 (Open Shortest Path First Version 3) debug flags. If logging is enabled, results are sent to the logging system.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`[ no ] debug ipv6 ospf all`

no

Disable all OSPFv3 debug flags.

Usage Guidelines

Use this command to enable or disable all OSPFv3 debug flags.

Example

The following command disables all OPSFv3 debug flags enabled by any of the **debug ip ospf** commands:

```
no debug ipv6 ospf all
```

The following command enables all OSPFv3 debug flags:

```
debug ipv6 ospf all
```

debug ipv6 ospf event

Enables or disables debugging of OSPFv3 protocol events. If logging is enabled, results are sent to the logging system. If no keywords are specified, all events are enabled for debugging.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

```
[ no ] debug ipv6 ospf event [ abr | asbr | os | router ]
```

no

Disables debugging the specified OSPFv3 event. If no keywords are specified, all events are disabled.

abr

Enables debugging of Area Border Router (ABR) events.

asbr

Enables debugging of Autonomous System BOundary Router (ASBR) events.

os

Enables debugging of operating system (OS) events.

router

Enables debugging of router events.

Usage Guidelines

Use this command to output debug information for OSPFv3 events.

Example

To enable all event debug information, enter the following command;

```
debug ipv6 ospf event
```

To disable all event debug information, enter the following command;

```
no debug ipv6 ospf event
```

debug ipv6 ospf ifsm

Enables or disables OSPFv3 Interface State Machine (ISM) troubleshooting, based on ISM information type. If no keywords are specified all ISM information types are enabled. If logging is enabled, results are sent to the logging system.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

```
[ no ] debug ipv6 ospf ism [ events | status | timers ]
```

no

Disables debugging the specified ISM information. If no keywords are specified, all information is disabled.

events

Enables debugging ISM event information.

status

Enables debugging ISM status information.

timers

Enables debugging ISM timer information.

Usage Guidelines Use this command to output ISM debug information.

Example

To enable all ISM debug information, enter the following command;

```
debug ipv6 ospf ism
```

To disable all ISM debug information, enter the following command;

```
no debug ipv6 ospf ism
```

debug ipv6 ospf lsa

Enables or disables troubleshooting on OSPFv3 Link State Advertisements (LSAs), based on the specific LSA option. If no keywords are specified, all options are enabled. If logging is enabled, results are sent to the logging system.

Product PDSN

HA

GGSN

Privilege Security Administrator, Administrator, Operator

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
[ no ] debug ip ospf lsa [ flooding | generate | install | maxage | refresh
 ]
```

no

Disables the specified LSA debug information. If no keyword is specified, all LSA debug information is disabled.

flooding

Enables LSA flooding information.

generate

Enables LSA generation information.

install

Enables LSA install information.

maxage

Enables LSA maximum age information in seconds. The maximum age is 3600 seconds.

refresh

Enables LSA refresh information.

Usage Guidelines

Use this command to output debug information for LSAs.

Example

To enable all LSA debug information, enter the following command;

```
debug ipv6 ospf lsa
```

To disable all LSA debug information, enter the following command;

```
no debug ipv6 ospf lsa
```

debug ipv6 ospf nsm

Enables or disables troubleshooting OSPFv3 Neighbor State Machines (NSMs), based on the specific NSM information type. If no keyword is specified, all NSM information types are enabled. If logging is enabled, results are sent to the logging system.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
[ no ] debug ipv6 ospf nsm [ interface | redistribute ]
```

no

Disables the debugging the specified NSM information type. If no keyword is specified, all information types are disabled.

interface

Enables debugging NSM on this interface.

redistribute

Enables debugging NSM redistribution information.

Usage Guidelines Use this command to output debug information for OSPFv3 NSMs

Example

To enable all NSM debug information, enter the following command;

```
debug ipv6 ospf nsm
```

To disable all NSM debug information, enter the following command;

```
no debug ipv6 ospf nsm
```

debug ipv6 ospf packet

Enables or disables troubleshooting of specific OSPFv3 packet information. If logging is enabled, results are sent to the logging system.

Product PDSN

HA

GGSN

Privilege Security Administrator, Administrator, Operator

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
[ no ] debug ipv6 ospf packet { dd | hello | ls-ack | ls-request |
ls-update } [ recv | send ] [ detail ]
```

no

Disable debugging of the specified packet information.

dd

Enables debugging database descriptions.

hello

Enables debugging hello packets.

ls-ack

Enables debugging link state acknowledgements.

ls-request

Enables debugging link state requests.

ls-update

Enables debugging link state updates.

recv

Enables debugging only on received packets.

send

Enables debugging only on sent packets.

detail

Enables detailed information in the debug output.

Usage Guidelines

Use this command to output specific OSPFv3 packet information.

Example

To enable all packet debug information, enter the following command;

```
debug ipv6 ospf packet all
```

To disable all route debug information, enter the following command;

```
no debug ipv6 ospf packet all
```

debug ipv6 ospf route

Sets the route calculation method to use in debugging OSPFv3 routes. If no route calculation method is specified, all methods are enabled. If logging is enabled, results are sent to the logging system.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
[ no ] debug ipv6 ospf route [ ase | ia | install | spf ]
```

no

Disables debugging of route information. If no keyword is specified all information types are disabled.

ase

Enables debugging information on autonomous system external (ASE) route calculations.

ia

Enables debugging information on Inter-Area route calculations.

install

Enables debugging information on route installation.

spf

Enables debugging information on Shortest Path First (SPF) route calculations.

Usage Guidelines Use this command to output debug information for OSPF routes.

Example

To enable all route debug information, enter the following command;

```
debug ipv6 ospf route
```

To disable all route debug information, enter the following command;

```
no debug ipv6 ospf route
```

default terminal

Restores the system default value for the terminal options.

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

```
default terminal { length | width }
```

length | width

length: Resets the terminal length to the system default.

width: Resets the system default terminal width.

Usage Guidelines Restore the default terminal settings when the current paging and display wraps inappropriately or pages to soon.

Example

The following sets the default length then width in two commands.

```
default terminal length
default terminal width
```

delete

Removes the specified file(s) permanently from the local.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

delete *filepath* **[-noconfirm]**

filepath

Specifies the location of the file to rename. The path must be formatted as follows:

For the ASR 5000:

[file:]{ /flash | /pcmcia1 | /hd-raid }[/*directory* **]/***file_name*

Important Use of the ASR 5000 SMC hard drive is not supported in this release.

For the ASR 5500:

[file:]{ /flash | /usb1 | /hd-raid }[/*directory* **]/***file_name*

For VPC:

[file:]{ /flash | /hd-raid / usb1 | usb2 | /cdrom1 }[/*directory* **]/***file_name*

Important The USB ports and CD-ROM must be configured via the hypervisor to be accessible.

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

-noconfirm

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

Important Use of the **-noconfirm** option should be done with extra care to ensure the file is specified accurately as there is no method of recovering a file that has been deleted.

Usage Guidelines Deleting files is a maintenance activity which may be part of periodic routine procedures to reduce system space utilization.

Example

The following removes files from the local */flash/pub* directory.

```
delete /flash/pub/june03.cfg
```

delete support record

Removes a Support Data Record (SDR) with s specified record-id or all SDRs in the specified range of record-ids.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description **delete support record** *<record-id>* **[to** *<record-id>* **]**

record-id

Specifies a single SDR as an integer from 0 to 65536.

Each SDR is identified by a time index called the record-id. For example, the most recent record is always record-id 0 (filename = sdr.0.gz). The next older record is record-id 1 (filename = sdr.1.gz), and so on.

to *record-id*

Specifies the endpoint record-id when deleting a range of SDRs.

Usage Guidelines Use this command to delete one or more SDRs stored on the system. For additional information on the Support Data Collector feature, refer to the *System Administration Guide*.

Example

The following command deletes the SDR with a record-id of 5 (filename = sdr.5.gz):

```
delete support record 5
```

dhcp force

Tests the lease-renewal for DHCP-assigned IP addresses for a particular subscriber.

Product

GGSN

ASN-GW

P-GW

SAEGW

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

dhcp force lease-renewal { callid *id* **| imsi** *imsi* **[nsapi** *nsapi* **] | msid** *msid* **}**

callid *id*

Clears the call ID specified as a 4-byte hexadecimal number.

imsi *msid*

Disconnects the subscriber with the specified msid. The IMSI (International Mobile Subscriber Identity) ID is a 50-bit field which identifies the subscriber's home country and carrier. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes ('). For example; '$'.

nsapi *nsapi*

Specifies a Network Service Access Point Identifier (NSAPI) an integer from 5 to 15.

msid *id*

Disconnects the mobile user identified by *ms_id*. *ms_id* must be from 7 to 16 digits specified as an IMSI, MIN, or RMI. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes ('). For example; '$'.

Usage Guidelines

Use this command tests a forced IP address lease renewal for a specific subscriber.

Example

The following command tests DHCP lease renewal for a subscriber with an MSID of *1234567*:

```
dhcp force lease-renewal msid 1234567
```

dhcp test

Tests DHCP (Dynamic Host Configuration Protocol) functions for a particular DHCP service.

Product

GGSN

ASN-GW

P-GW

SAEGW

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
dhcp test dhcp-service svc_name [ all | server ip_address ]
```

dhcp-service *svc_name*

Specifies the name of the DHCP service as an alphanumeric string of 1 through 63 characters that is case sensitive.

all

Tests DHCP functionality for all servers.

server *ip_address*

Tests DHCP functionality for the server specified by an IP address entered using IPv4 dotted-decimal notation.

Usage Guidelines

Once DHCP functionality is configured on the system, this command can be used to verify that it is configured properly and that it can successfully communicate with the DHCP server.

Executing this command causes the system to request and allocate an IP address and then release it.

If a specific DHCP server is not specified, then each server configured in the service is tested.

Example

The following command tests the systems ability to get an IP address from all servers a DHCP service called *DHCP-Gi* is configured to communicate with:

```
dhcp test dhcp-service DHCP-Gi all
```

diameter disable endpoint

Disables a Diameter endpoint without removing the peer's configuration.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

diameter disable endpoint *endpoint_name* **peer** *peer_id*

endpoint_name

Specifies the endpoint in which the peer is configured as an alphanumeric string of 1 through 63 characters.

peer *peer_id*

Specifies the Diameter peer host name to be disabled as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to administratively disable a Diameter peer without removing the peer configuration. This command will tear down all connections on the specified peer (by sending a DPR if the configuration demands the same at peer level configuration). The peer will remain in disabled state until it is enabled again. Also see the **diameter enable endpoint** command.

Example

This command disables the Diameter peer *peer12*:

```
diameter disable endpoint endpoint1 peer peer12
```

diameter enable endpoint

Enables a Diameter endpoint that is disabled.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

diameter enable endpoint *endpoint_name* **peer** *peer_id*

endpoint_name

Specifies the endpoint in which the peer is configured as an alphanumeric string of 1 through 63 characters.

peer *peer_id*

Specifies the Diameter peer host name to be enabled as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to administratively enable a Diameter peer. Also see the **diameter disable endpoint** command.

Example

This command enables the Diameter peer *peer12*:

```
diameter enable endpoint endpoint1 peer peer12
```

diameter-proxy conn-audit

This command enables the Diameter proxy Peer Connection Status Audit with Diabase clients.

Product

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
diameter-proxy conn-audit interval 1-10
default diameter-proxy conn-audit
```

default

Configures the default setting.

By default, Diameter proxy Peer Connection Status Audit with Diabase clients is disabled.

diameter-proxy

Specifies the Diameter proxy related configurations.

conn-audit

Specifies the periodic connection status audit processes. Disabled by default.

interval *1-10*

Specifies the connection status audit interval in minutes, in the range of 1 through 10. Recommended value is 2 minutes.

Usage Guidelines

Enabling Diamproxy Peer Connection Status Audit with Diabase clients might affect performance of the services using Diameter interface. Service is impacted only when auto-correction happens (due to mismatch) and the cases are:

1. When Diabase state is IDLE and Diameter proxy is OPEN.
2. When Diabase state is OPEN and Diameter proxy is IDLE.

In both these cases, Diabase corrects the connection status based on information received in audit message. Diameter messaging failures is avoided once Diabase corrects the connection status.

Example

The following command specifies that the connection status audit interval is *2*minutes:

```
diameter-proxy conn-audit interval 2
```

diameter reset connection

Resets individual TCP/SCTP connections for a specified Diameter endpoint.

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

`diameter reset connection { endpoint` *`endpoint_name`* **`peer`** *`peer_id`* **`}`**

endpoint *endpoint_name*

Resets connection to the endpoint specified as an alphanumeric string of 1 through 63 characters.

peer *peer_id*

Resets connection to the Diameter peer host name specified as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to reset the TCP/SCTP connections for the specified endpoint/peer. With this command, the connection will be closed temporarily after DPR/DPA. If there is any traffic to be sent to the particular peer, then the connection will be re-established.

This command overrides the endpoint configured in any other configuration mode.

This command is applicable only when the specified peer is enabled.

Example

This command resets connection to the endpoint named *test123*:

```
diameter reset connection endpoint test123
```

diameter reset route failure

Resets the failed route status of a Diameter destination-host combination via peer to AVAILABLE status.

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

`diameter reset route failure [ endpoint` *`endpoint_name`* **`] [ host`** *`host_name`* **`] [ peer`** *`peer_id`* **`]`**

endpoint *endpoint_name*

Resets paths to the endpoint specified as an alphanumeric string of 1 through 63 characters.

host *host_name*

Resets the FAILED status of all Diameter destination-host combination routes via peer for every Diameter client within the chassis having a specific host name to AVAILABLE.

Specifies the Diameter host name as an alphanumeric string of 1 through 63 characters.

peer *peer_id*

Resets the FAILED status of all Diameter destination-host combination routes via a peer having specific peer-Id for every Diameter client within the chassis to AVAILABLE.

Specifies the Diameter peer host name as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to reset the FAILED status of all Diameter destination-host combination routes via peer for every Diameter client within the chassis to AVAILABLE status.

This command also resets the failure counts used to determine the AVAILABLE/FAILED status of a destination-host combination.

When executed from local context, this command matches all contexts. If an optional keyword is not supplied, a wildcard is used for the value.

The status of every matching combination of destination-host via peer for every matching Diameter client within the chassis will be reset to AVAILABLE. The failure counts that are used to determine AVAILABLE/FAILED status will also be reset.

Also see the **route-entry** and **route-failure** commands in the *Diameter Endpoint Configuration Mode Commands* chapter.

Default value: N/A

Example

The following command resets the FAILED status of all Diameter destination-host combination routes via peer for every Diameter client within the chassis for specified endpoint name to AVAILABLE.

```
diameter reset route failure endpoint endpoint123
```

directory

Lists the files in a specified location.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

directory *filepath* **[-size] [-reverse] [-time]**

filepath

Specifies the directory path to list the contained files using the following format:

For the ASR 5000:

[file:]{ /flash | /pcmcia1 | /hd }[/*directory* **]/***file_name*

Important Use of the ASR 5000 SMC hard drive is not supported in this release.

For the ASR 5500:

[file:]{ /flash | /usb1 | /hd }[/*directory* **]/***file_name*

For VPC:

[file:]{ /flash | /hd-raid | /usb1 | /usb2 | cdrom1 }[/*directory* **]/***file_name*

Important The USB ports and CD-ROM must be configured via the hypervisor to be accessible.

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

-size

Indicates the size of each file should be displayed in the output.

-reverse

Indicates the order of files listed should be in descending order (z-aZ-A9-0). Default is to sort in ascending order (0-9A-Za-z).

-time

Indicates the last modification timestamp of each file should be displayed in the output.

Usage Guidelines

Lists such things as log and crash files from multiple nodes within the network.

The optional arguments may be specified individually or in any combination.

Example

The following command will list the files in the local */flash/pub* directory sorted in reverse order.

```
directory /flash/pub -reverse
```

disable radius

Prevents the system from making requests of a selected RADIUS server.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

disable radius { [charging] [accounting] server *ipv4/ipv6_address* **[group** *group_name* **| port** *port_number* **+] }**

[charging] [accounting]

Specifies the type of RADIUS server to disable.

- **accounting**: Specifies accounting servers
- **charging**: Specifies charging servers
- **charging accounting**: Specifies charging accounting servers

server *ipv4/ipv6_address*

Specifies the RADIUS server by IP address entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

port *port_number*

Specifies the port number of the RADIUS server being disabled an integer from 0 through 65535. Default: 1812 (authentication) 1813 (accounting)

group *group_name*

Specifies the RADIUS group to which the server belongs as an alphanumeric string of 1 through 63 characters. Use this option in the event that the RADIUS server belongs to multiple groups and you only want to disable the server within the specific group. Default: **default**

Usage Guidelines

Use this command to gracefully stop the system from making requests of a specific RADIUS server.

Example

The following command disables a RADIUS accounting server with an IP address of *209.165.200.229* , the default accounting server port number, and that resides in the *Group5* server group:

```
disable radius accounting server 209.165.200.229
 group Group5
```

dns-client

Performs DNS (Domain Name System) query on the basis of specified DNS client name, DNS query domain name, and type of query criteria.

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

dns-client *dns_client_name* **[query-type { A | AAAA | NAPTR | SRV }] query-name** *query_domain_name*

dns-client *dns_client_name*

Specifies the name of the DNS client whose cache and/or statistics are to be queried. It must be an existing DNS client expressed as an alphanumeric string of 1 through 64 characters.

query-type { A | NAPTR | SRV }]

Specifies that the type of query to perform for the defined DNS client is to be displayed.

- **A**: Filters DNS results based on domain IPv4 address records (A records). This is the default query type.
- **AAAA**: Filters DNS results based on domain IPv6 address records (AAAA records).
- **NAPTR**: Filters DNS results based on Naming Authority Pointer records (NAPTR).
- **SRV**: Filters DNS results based on service host records (SRV records).

query-name *query_domain_name*

Filters the DNS results based on the query domain name expressed as an alphanumeric string of 1 trough 255 characters.

query_domain_name is the domain name used to perform the DNS query and is different from the actual domain name which is resolved. For example, to resolve the SIP server for *service.com*, the query name is *_sip._udp.service.com* and the query type is **SRV**.

Usage Guidelines

Use this command to perform DNS query on the basis of DNS Client name and filters the query results based on query type and query name. This command also populates the result into DNS Cache. This command used the current context to DNS request.

Example

The following command displays statistics for a DNS client named *test_dns* with query type for IP address as *A* and query name as *domain1.com*:

```
dns-client test_dns query-type A query-name domain1.com
```

egtpc test echo

Tests the ability of a GGSN/P-GW service to exchange GTP-C echo request messages with specified peer(s).

Product

GGSN

P-GW

SAEGW

Privilege

Operator, Config-Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

egtpc test echo gtp-version *version* **src-address** *ip_address* **{ all | peer-address** *ip_address* **}**

gtp-version *version*

Specifies version number for sending Echo request message.

version must be an integer from 0 through 2.

Important If peer is not a new peer for service bind to **src-address**, then echo request is sent with the last known highest version of the peer.

src-address *ip_address*

Specifies the IP address of a Gn interface configured on the system.

ip_address must be entered using IPv4 dotted-decimal notation or IPV6 colon-separated-hexadecimal notation.

Important The IP address of the system's Gn interface must be bound to a configured GGSN/P-GW service prior to executing this command.

all

Sends GTP-C echo requests to first 100 peers that currently have sessions with the GGSN/P-GW service.

Important If this keyword is selected, additional confirmation is required after the following message, "Warning: Due to possibility of huge number of connected peers, considering system performance impacts, issue echo request to only 100 peers".

peer-address *ip_address*

Specifies that GTP-C echo requests will be sent to a specific peer.

ip_address must be entered using IPv4 dotted-decimal notation or IPV6 colon-separated-hexadecimal notation.

Usage Guidelines

This command tests the GGSN's or P-GW's ability to exchange GPRS Tunneling Protocol control plane (GTP-C) packets with the specified peer. This command is useful for troubleshooting and/or monitoring.

This command must be executed from within the context in which the GGSN/P-GW service is configured.

Important In StarOS v14.0 and later, this command replaces the **gtpv0 test echo** and **gtpc test echo** commands.

Example

The following command issues GTP-C echo packets from a GGSN service bound to address *192.168.157.43* to an SGSN with an address of *192.168.1.52*:

```
egtpc test echo gtp-version 1 src-address 192.168.157.43 peer-address
192.168.1.52
```

enable radius

Enables the system to start making requests of a specific RADIUS server.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

enable radius { [charging] [accounting] server *ipv4/ipv6_address* **[group** *group_name* **| port** *port_number* **+] }**

[charging] [accounting]

Specifies the type of RADIUS server to enable.

- **accounting**: Specifies accounting servers
- **charging**: Specifies charging servers
- **charging accounting**: Specifies charging accounting servers

server *ipv4/ipv6_address*

Specifies the RADIUS server by an IP address entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

port *port_number*

Specifies the port number of the RADIUS server being enabled as an integer from 0 through 65535. Default: 1812 (authentication) 1813 (accounting)

group *group_name*

Specifies the RADIUS group to which the server belongs as an alphanumeric string of 1 through 63 characters. Use this option in the event that the RADIUS server belongs to multiple groups and you only want to disable the server within the specific group. Default: **default**

Usage Guidelines

Use this command to allow the system to start making requests of a specific RADIUS server.

Example

The following command enables a RADIUS accounting server with the IP address *209.165.200.229* , the default accounting server port number, and in the *Group5* server group:

```
enable radius accounting server 209.165.200.229 group Group5
```

exit

Terminates the current CLI session.

Product

All

Privilege

Any

Syntax Description

exit

Usage Guidelines

Use this command to terminate the current CLI session.

filesystem

Use this command to check, format or repair the filesystem on internal and external storage devices.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]`*host_name*`#`

Syntax Description

For the ASR 5000:

filesystem { check | format | repair | synchronize } { /flash | /pcmcia1 | /hd-raid } [card *slot_num* **]**

For the ASR 5500:

filesystem { check | format | repair | synchronize } { /flash | /usb1 | /hd-raid } [card *slot_num* **]**

For VPC:

filesystem { check | format | repair | synchronize | update } { /flash | /hd-raid | /usb1 | /usb2 | cdrom1 }

The following devices are supported based on platform type:

- **/flash** – ASR 5x00, VPC
- **/hd-raid** – ASR 5x00, VPC
- **/pcmcia1** – ASR 5000 only
- **/usb1** – ASR 5500, VPC (if configured via hypervisor)
- **/usb2** – VPC (if configured via hypervisor)
- **/cdrom1** – VPC (if configured via hypervisor)

Important For VPC, the USB ports and CD-ROM must be configured via the hypervisor to be accessible by the Control Function (CF) virtual machine.

check

Checks for filesystem corruption.

format

Reformats file system.

Caution This keyword erases all data on the device.

Formatting /flash will remove all boot configurations and the ASR 5x00 chassis-ID. Before running format, be sure to review or save the output of the **show boot** command. After running **format**, be sure to restore boot entries as needed, generate a new chassis-ID, and execute **save configuration** to save the running configuration.

repair

Repairs file system corruption.

synchronize

See the description of the **filesystem synchronize** command for detailed information. **Not supported on VPC-SI.**

update

Updates the boot code on the file system. **Supported on VPC-SI only.**

Usage Guidelines

Check, format, or repair all directories and files from on an internal or external storage device and re-establish the file system.

Example

The following command formats the PCMCIA card located in slot 1 on the SMC (ASR 5000):

```
filesystem format /pcmcia1
```

filesystem synchronize

Use this command to synchronize the file systems of active and standby storage devices on MIO card or VPC-DI Control Function (CF) virtual machines.

Product

All

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

For the ASR 5500:

filesystem synchronize [/flash | /usb1 | all] [checkonly] [from *card_num* **| to** *card_num* **] [-noconfirm]**

For VPC:

filesystem synchronize [/flash | /usb1 | /usb2 | cdrom1 | all] [checkonly] [from *card_num* **| to** *card_num* **] [-noconfirm]**

The following devices are supported based on platform type:

- **/flash** – ASR 5x00, VPC
- **/hd-raid** – ASR 5x00, VPC
- **/usb1** – ASR 5500, VPC (if configured via hypervisor)
- **/usb2** – VPC (if configured via hypervisor)
- **/cdrom1** – VPC (if configured via hypervisor)
- **all** – Selects all file systems

checkonly

Checks for file system corruption; does not modify file systems.

[from *card_num* | to *card_num*]

Copies files from a source card to a destination card specified by slot numbers.

-noconfirm

Executes the command without displaying "are you sure" prompts.

Usage Guidelines

Synchronize the file systems between active and standby storage devices.

Example

The following command all file systems on the management card:

```
filesystem synchronize all
```

The following command sequence appears when **filesystem synchronize /flash** is run after **save configuration /flash/***filename* **-redundant** is executed and a change has been made to the configuration:

```
filesystem synchronize /flash
2 to be updated on card 2
   /flash/oam.cfg
   /flash/service.cfg
0 to be updated (but are newer) on card 2
```

```
0 to be deleted on card 2
Are you sure? [Yes|No]:
```

You must confirm the synchronization before it will be initiated.

If "No files to update" appears, you are returned to the CLI prompt.

gtpc test echo

Tests the ability of a GGSN service to exchange GTP-C echo request messages with the specified SGSN(s).

Product

GGSN

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`gtpc test echo src-address` *`gn_address`* **`{ all | sgsn-address`** *`ip_address`* **`}`**

src-address *gn_address*

Specifies the IP address of a Gn interface configured on the system in IPv4 dotted-decimal notation.

Important The IP address of the system's Gn interface must be bound to a configured GGSN service prior to executing this command.

all

Specifies that GTP-C echo requests will be sent to all SGSNs that currently have sessions with the GGSN service.

sgsn-address *ip_address*

Specifies that GTP-C echo requests will be sent to a SGSN specified by an IP address in IPv4 dotted-decimal notation.

Usage Guidelines

This command tests the GGSN's ability to exchange GPRS Tunneling Protocol control plane (GTP-C) packets with the specified SGSNs. This command is useful for troubleshooting and/or monitoring.

This command must be executed from within the context in which the GGSN service is configured.

Refer also to the **gtpu test** command.

Important In StarOS v14.0 and later, this command has been replaced by the **egtpc test echo** command.

Example

The following command issues GTP-C echo packets from a GGSN service bound to address *192.168.157.32* to an SGSN with an address of *192.168.157.2*:

```
gtpc test echo src-address 192.168.157.32 sgsn-address 192.168.157.2
```

gtpp interim now

Check points current GTPP accounting messages and identifies which types of interim CDRs are to be generated and sent to the external charging/storage servers (for example, a CFG or a GSS). The impact of this command is immediate.

Product

GGSN

SGSN

SGW

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

gtpp interim now [active-charging egcdr | apn *apn_name* **| callid** *call_id* **| cdr-types { gcdr | mcdr | scdr } | dhcp-server** *ip_address* **| gprs-service** *svc_name* **| ggsn-address** *ggsn_ip_addr* **| ggsn-service** *svc_name* **| imsi** *imsi* **[ip-address** *sub_address* **[username** *name* **]] | ip-address***sub-address* **| nsapi** *nsapi* **[ip-address** *sub-address* **[username** *name* **]] | ip-pool** *pool_name* **| mcc** *mcc_number* **mnc** *mnc_number* **| msisdn** *msisdn_num* **| sgsn-address** *ip_address* **| sgsn-service** *svc_name* **| username** *name* **] +**

active-charging

This feature is specific to the GGSN and is documented separately. .

apn *apn_name*

Initiates GTPP interim accounting for all PDP contexts accessing the APN specified as an alphanumeric string of 1 through 62 characters that is case sensitive.

callid *call_id*

Identifies a specific call id as an 8-digit hexadecimal number.

cdr-types { mcdr | scdr }

Specifies the CDR types to be generated by the SGSN:

gcdr - Instructs the GGSN to only generate G-CDRs.

mcdr - Instructs the SGSN to only generate M-CDRs

scdr - Instructs the SGSN to only generate S-CDRs.

This keyword is specific to the SGSN.

dhcp-server *ip_address*

Identifies the DHCP server where the IP address (defined with the **ip address** keyword) was allocated by the IP address of the DHCP server entered using IPv4 dotted-decimal notation.

ggsn-address *ggsn_ip_addr*

Specifies the IP address of the interface to the GGSN using IPv4 dotted-decimal notation. This keyword is specific to the GGSN.

ggsn-service *svc_name*

Initiates GTPP interim accounting for all PDP contexts currently being facilitated by the GGSN service specified as an alphanumeric string of 1 through 63 characters that is case sensitive. This keyword is specific to the GGSN.

gprs-service *svc_name*

Initiates GTPP interim accounting for all PDP contexts currently being facilitated by an existing GPRS service specified as an alphanumeric string of 1 through 63 characters that is case sensitive. This keyword is specific to the SGSN.

imsi *imsi* [ip-address *sub_address* [username *name*] | nsapi *nsapi* [ip-address *sub-address* [username *name*] | username *name*]]

Initiates GTPP interim accounting for a specific International Mobile Subscriber Identity (IMSI) number. The request could be further filtered using any of the following keywords:

- **ip-address**: Interim accounting will be performed for the IP address specified by *sub_address*. The command can be further filtered by specifying a specific username with that address.
- **nsapi**: Interim accounting will be performed for a Network Service Access Point Identifier (NSAPI) specified as an integer from 5 to 15. The command can be further filtered by specifying a specific ip address and/or a username with that address, or just a specific username.

ip-address *sub_address* [username *name*]

Initiates GTPP interim accounting for the IP address of the subscriber specified in IPv4 dotted-decimal notation.

The command can be further filtered by specifying a username with that address. The name is the subscriber's name and can be a sequence of characters and/or wildcard characters ('$' and '*') from 1 to 127 characters. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as wildcard enclose them in single quotes ('). For example; '$'.

ip-pool *pool_name*

Initiates GTPP interim accounting for all PDP contexts that were allocated IP addresses from an existing pool specified as an alphanumeric string of 1 through 31 characters that is case sensitive. This keyword is applicable to the GGSN only.

mcc *mcc_number* mnc *mnc_number*

mcc_number: Specifies the mobile country code (MCC) portion of the PLMN identifier and can be configured to any 3-digit integer value between 100 and 999.

mnc_number: Specifies the mobile network code (MNC) portion of the PLMN identifier and can be configured to any 2- or 3-digit integer between 00 and 999.

msisdn *msisdn_num*

Configures the SGSN to include the Mobile Subscribers Integrated Services Digital Network identifier in generated CDRs (M-CDRs and/or the S-CDRs). This keyword is applicable for SGSN only.

msisdn_number must be followed by a valid MSISDN number, consisting of 1 to 15 digits.

sgsn-address *ip_address*

Initiates GTPP interim accounting for all PDP contexts currently being facilitated by the SGSN specified by an IP address in IPv4 dotted-decimal notation. This keyword is specific to the GGSN.

sgsn-service *svc_name*

Initiates GTPP interim accounting for all PDP contexts currently being facilitated by an existing SGSN service specified an alphanumeric string of 1 through 63 characters that is case sensitive. This keyword is specific to the SGSN.

username *name*

Initiates GTPP interim accounting for all PDP contexts for the subscriber name specified as an alphanumeric string of 1 through 127 characters that is case sensitive.

+

More than one of the above keywords can be entered within a single command.

Usage Guidelines

This command causes GTPP accounting CDRs to immediately be generated for all active sessions that are in the current context. If executed within the local context, CDRs will be generated for all active sessions regardless of context. This command generates only certain types of CDRs including GCDRs, SGWCDRs, and SCDRs.

The sending of the CDRs is paced so as not to overload the accounting server.

Example

The following command causes CDRs to immediately be generated:

```
gtpp interim now
```

gtpp interim now active-charging egcdr

Check points current GTPP accounting messages for active charging immediately.

Product

GGSN

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

gtpp interim now active-charging egcdr [callid *call_id* **| imsi** *imsi* **| msid** *msid* **| rulebase** *rbase_name* **| session-id** *sess_id* **| username** *name* **]**

callid *call_id*

Initiates GTPP interim accounting for a session for the call ID specified as an 8-digit hexadecimal number.

imsi *imsi*

Initiates GTPP interim accounting for a International Mobile Subscriber Identity (IMSI) number. specified as a sequence of hexadecimal digits and wildcard characters - $ matches a single character and * matches multiple characters

msid *msid*

Initiates GTPP interim accounting for a Mobile Station Identifier (MSID) number specified as a sequence of up to 24 digits and wildcard characters - $ matches a single character and * matches multiple characters

rulebase *rbase_name*

Initiates GTPP interim accounting for sessions that use the named active charging rulebase specified as an alphanumeric string of 1 through 24 characters.

session-id *sess_id*

Initiates GTPP interim accounting for a current active charging session.

Usage Guidelines

This command causes GTPP accounting eG-CDRs to immediately be generated for active charging sessions that meet the specified criteria.

The sending of the CDRs is paced so as not to overload the accounting server.

username *name*

Initiates GTPP interim accounting for all PDP contexts for the subscriber name specified as an alphanumeric string of 1 through 127 characters that is case sensitive.

Example

The following command causes eG-CDRs to immediately be generated for active charging sessions using the rulebase named rulbase1:

```
gtpp interim now active-charging egcdr rulebase rulebase1
```

gtpp storage-server commit

Causes the GTPP storage server to archive all buffered packets.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`gtpp storage-server commit now [ group name` *`group_name`* **`]`**

group name *group_name*

Commits Storage Server for an existing group name expressed as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

This command sends a request to the GTPP Storage Server to archive all buffered packets. It also deletes all CDRs that have been acknowledged by the charging gateway function (CGF). The deleted CDRs are saved in a separate file.

Note that this command must be executed from within the context in which the GTPP Storage Server is configured.

Refer to the **gtpp storage-server** command in the *Context Configuration Mode Commands* chapter for more information.

gtpp storage-server streaming start

This command enables to start streaming of the copied CDR files from active chassis when the ICSR switchover occurs.

Product

Important This command is obsolete in release 16.0. In 16.0 and later releases, use the "**gtpp push-to-active url**" CLI command in global configuration mode to enable the automatic transfer of stranded CDRs to active chassis.

GGSN

P-GW

S-GW

SGSN

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

gtpp storage-server streaming start [group name *group_name* **]**

group name *group_name*

Specifies the name of a GTPP group configured in the current context as an alphanumeric string of 1 through 63 characters.

Note that, if the group name is not specified, then all the GTPP groups in the current context will be considered. If the group name is specified, then only the group provided in this CLI command will be considered.

Usage Guidelines

This command is used to resynchronize the CDRs left on local HDD with the active GTPP' streaming feed to transfer the CDRs from active chassis to IT mediation device during ICSR switchover.

Note that this CLI command must be executed from within the context in which the GTPP Storage Server is configured.

In the event of ICSR switchover, to transfer the copied CDRs from active chassis to IT mediation device, follows these steps:

1. Manually copy files from old active chassis to new active chassis.
2. Issue this CLI command "**gtpp storage-server streaming start**" to start streaming of the copied files from active chassis.
3. If the streaming is in progress, then wait till the current file is fully streamed out. After the current file is fully streamed out, then rebuild the file list (to get the copied CDR files) and start streaming based on the timestamp.
4. If the streaming is not in progress then rebuild the file list (to get the copied CDR files) and start streaming.

gtpp test

Tests communication with configured Charging Gateway Function (CGF) servers or a GTPP Storage-Server.

Product

ePDG

GGSN

P-GW

SAEGW

SGSN

Privilege

Operator, Config-Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

gtpp test { accounting { all | cgf-server *ipv4/ipv6_address* **[port** *port_num* **] | group name** *group_name* **} | storage-server [address** *ipv4/ipv6_address* **port** *udp-port* **| group name** *group_name* **] }**

all

Tests all CGFs configured within the given context.

cgf-server *ipv4/ipv6_address* [port *port_num*]

Tests a CGF configured within the given context and specified by the IP address of the CGF entered using IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.

port *port_num*: Specifies the port number of CGF server. The port number must be an integer ranging from 1 to 65535.

This optional keyword is introduced to ease the identification of product specific CDRs. This configuration provides the flexibility to send ePDG, SaMOG and P-GW LBO CDRs to the same CGF server on different ports.

When the port is specified, this command displays the status of CGF server with the specified IP address and port. If port is not provided then it will show the status of all CGF servers with the specified IP address.

group name *group_name*

Tests the storage server for an existing group name specified as an alphanumeric string of 1 through 63 characters.

storage-server [address *ipv4/ipv6_address* port *udp-port*]

Tests the connectivity and provides round trip time for the echo request sent to the GTPP Storage-Server configured in the requested context. The IP address of the GSS is entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation and the UDP port is the one defined for the GTPP Storage Server.

Usage Guidelines

This command is used to verify the configuration of and test the system's ability to communicate with one or all configured GSS/CGFs for monitoring or troubleshooting purposes.

When executed, this command causes the system to send GTPP echo packets to the specified GSS/CGF(s). The command's response will display whether the GSS/CGF is active or unreachable.

Example

The following command tests communication with a CGF server having an IP address of *209.165.200.224*:

```
gtpp test accounting cgf-server 209.165.200.224
```

The following command tests communication with a GSS configured in requested context:

```
gtpp test storage-server
```

The following command verifies the communication with a GSS having an IP address of *209.165.201.0* and port *50000*, without configuring it in a context:

```
gtpp test storage-server address 209.165.201.0 port 50000
```

gtpu test echo

Tests the ability of a GGSN/P-GW/SAEGW/SGSN/S-GW service to exchange GTP-U echo request messages with specified peer(s).

Product

GGSN

P-GW

SAEGW

SGSN

S-GW

Privilege

Operator, Config-Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

StarOS v12.x and earlier:

gtpu test echo src-address *gn_address* **{ all | sgsn-address** *ip_address* **}**

StarOS v14.0 and later:

gtpu test echo gtpu-service *service_name* **{ all | peer-address** *ip_address* **} [gtpu-version { 0 | 1 }]**

src-address *gn_address*

Specifies the IP address of a Gn interface configured on the system using IPv4 dotted-decimal notation.

Important The IP address of the system's Gn interface must be bound to a configured GGSN service prior to executing this command.

all

Sends GTP-U echo requests to all SGSNs that currently have sessions with the GGSN service.

sgsn-address *ip_address*

Sends GTP-U echo requests to an SGSN specified by its IP address in IPv4 dotted-decimal notation.

gtpu-service *service_name*

Specifies an existing GTP-U service.

service_name is an alphanumeric string of 1 through 63 characters.

all

Sends GTP-U echo requests to first 100 peers that currently have sessions with the GTP-U service.

Important If this keyword is selected, additional confirmation is required after the following message, "Warning: Due to possibility of huge number of connected peers, considering system performance impacts, issue echo request to only 100 peers".

peer-address *ip_address*

Specifies that GTP-U echo requests will be sent to a specific peer.

ip_address must be entered using IPv4 dotted-decimal notation or IPV6 colon-separated-hexadecimal notation.

gtpu-version { 0 | 1 }

Optional. Specifies the GTP-U version in which the test echo will be sent. **0** Specifies GTP-U version 0, and **1** specifies GTP-U version 1.

- If the GTP-U version of the peer is unknown, the GGSN/P-GW/SAEGW/SGSN/S-GW will use the user-configured GTP-U version.
- If the GTPU version of peer node is already known, the test echo is sent in the known GTP-U version.
- If the GTP-U version is not configured, and the peer version is unknown, the test echo is sent in GTP-U version 0.

Usage Guidelines

This command tests the GGSN/P-GW/SAEGW/SGSN/S-GW's ability to exchange GPRS Tunneling Protocol user plane (GTP-U) packets with the specified SGSNs/peer(s). This command is useful for troubleshooting and/or monitoring.

Important This command returns statistics on the number of packets transmitted and received; however, statistics are displayed right after transmitting the "echo" packet, but before receiving the response. Therefore, received statistics are always off by one. For more information, the same command should be run twice.

For example:

```
[ingress]asr5000# gtpu test echo gtpu-service sgw_ingress_gtpu peer-address 209.165.200.224
 gtpu-version 1
GTPU test echo
--------------
PEER: 209.165.200.224 Tx/Rx: 1/0 RTT(ms): 0 Recovery

[ingress]asr5000#
[ingress]asr5000# gtpu test echo gtpu-service sgw_ingress_gtpu peer-address 209.165.200.224
 gtpu-version 1
GTPU test echo
--------------
PEER: 209.165.200.224 Tx/Rx: 2/1 RTT(ms): 4285432 (COMPLETE)
```

Refer also to the **gtpc test** command.

Example

The following command issues GTP-U echo packets from a GGSN service bound to address *209.165.200.239* to an SGSN with an address of *209.165.200.243*:

```
gtpu test echo src-address 209.165.200.239 sgsn-address 209.165.200.243
```

The following command issues GTP-U echo packets from a GTP-U service named *gtpu_1* to the first 100 connected peers:

```
gtpu test echo gtpu-service gtpu_1 all
```

gtpv0 test echo

Tests the ability of a GGSN service to exchange GTPv0 echo request messages with the specified SGSN(s).

Product

GGSN

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

`gtpv0 test echo src-address` *`gn_address`* **`{ all | sgsn-address`** *`ip_address`* **`}`**

src-address *gn_address*

Specifies the IP address of a Gn interface configured on the system using IPv4 dotted-decimal notation.

Important The IP address of the system's Gn interface must be bound to a configured GGSN service prior to executing this command.

all

Sends GTPv0 echo requests to all SGSNs that currently have sessions with the GGSN service.

sgsn-address *ip_address*

Sends GTPv0 echo requests to an SGSN specified by its IP address in IPv4 dotted-decimal notation.

Usage Guidelines

This command tests the GGSN's ability to exchange GPRS Tunneling Protocol version 0 (GTPv0) packets with the specified SGSNs which can be useful troubleshooting and/or monitoring.

This command must be executed from within the context in which the GGSN service is configured.

Refer also to the **gtpc test** and **gtpu test** commands.

Important In StarOS v14.0 and later, this command has been replaced by the **egtpc test echo** command.

Example

The following command issues GTPv0 echo packets from a GGSN service bound to address *192.168.1.33* to an SGSN with an address of *192.168.1.42*:

```
gtpv0 test echo src-address 192.168.1.33 sgsn-address 192.168.1.42
```

hd raid

Performs RAID management operations on the platform's hard disk drives.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

For the ASR 5000:

```
hd raid { check | create { local1 | remote1 } | insert { local1 | remote1
 } | overwrite { local1 | remote1 } | directory pathname | limit number_files
 | mtime minutes } | remove { local1 | remote1 } | select { local1 | remote1
 } }  [ -force ] [ -noconfirm ]
```

For the ASR 5500:

```
hd raid { check | create { hd13 | hd14 | hd15 | hd16 | hd17 | hd18 } |
insert { hd13 | hd14 | hd15 | hd16 | hd17 | hd18} | overwrite { hd13 |
hd14 | hd15 | hd16 | hd17 | hd18 } | quarantine { directory pathname | limit
 number_file | mtime minutes } | remove { hd13 | hd14 | hd15 | hd16 | hd17 |
 hd18 } }  [ -force ] [ -noconfirm ]
```

For VPC:

```
hd raid { check | create | insert | overwrite | quarantine { directory
pathname | limit number_files | mtime minutes } | remove | select } { local1 |
local2 } [ -force ] [ -noconfirm ]
```

check

Starts a background check on RAID disks unless the RAID is running in degraded mode.

create { local1 | remote1 }

On the ASR 5000, creates a new RAID that could run in degraded mode on the specified drive:

- **local1** specifies the RAID is to be established on the primary SMC.
- **remote1** specifies the RAID is to be established on the backup SMC.

create *hd_num*

On the ASR 5500, creates a new RAID that could run in degraded mode on the hard drive array of a specific FSC.

hd_num specifies the RAID is to be established. *hd_num* corresponds to the FSC in slot numbers as shown below:

- hd13 = disk in slot 13
- hd14 = disk in slot 14
- hd15 = disk in slot 15
- hd16 = disk in slot 16
- hd17 = disk in slot 17
- hd18 = disk in slot 18

create { local1 | local2 }

On VPC, creates a new virtual RAID as vHD Local1 or vHD Local2.

insert { local1 | remote1 }

On the ASR 5000, inserts the specified disk to the running RAID causing it to recover from degraded mode.

- **local1** specifies the primary SMC is to be inserted into the RAID.
- **remote1** specifies the backup SMC is to be inserted into the RAID.

insert *hd_num*

On the ASR 5500, inserts the specified FSC disk array into the running RAID causing it to recover from degraded mode.

hd_num specifies the RAID is to be established. *hd_num* corresponds to the FSC in slot numbers as shown below:

- hd13 = disk in slot 13
- hd14 = disk in slot 14
- hd15 = disk in slot 15
- hd16 = disk in slot 16
- hd17 = disk in slot 17
- hd18 = disk in slot 18

insert { local1 | local2 }

On VPC, inserts the specified vHD into the running RAID causing it to recover from degraded mode.

overwrite { local1 | remote1 }

On the ASR 5000, overwrites the specified disk and adds it to the current running RAID to construct a fully mirrored array.

- **local1** specifies the primary SMC is to be inserted into the RAID.
- **remote1** specifies the backup SMC is to be inserted into the RAID.

overwrite *hd_num*

On the ASR 5500, overwrites the specified FSC disk array and adds it to the current running RAID to reconstruct the RAID 5 array.

hd_num specifies the RAID is to be established. *hd_num* corresponds to the FSC in slot numbers as shown below:

- hd13 = disk in slot 13
- hd14 = disk in slot 14
- hd15 = disk in slot 15
- hd16 = disk in slot 16
- hd17 = disk in slot 17
- hd18 = disk in slot 18

overwrite { local1 | local2 }

On VPC, overwrites the specified vHD and adds it to the current running RAID to construct a fully mirrored array.

quarantine [directory *pathname* | limit *number_files* | mtime *minutes*

Recovers and quarantines dirty-degraded RAID files.

- **directory** specifies the directory to which files are to be moved. *pathname* is expressed as an alphanumeric string of 1 through 29 characters. Default = "lost+found"
- **limit** sets the maximum number of files to quarantine. *number_files* is an integer from 0 to 1000000; 0 is unlimited. Default = 3000 (10 files per second within 5 minutes).
- **mtime** specifies within how many minutes the file is modified to be considered suspects for quarantine. *minutes* is an integer from 0 through 1440; 0 means no files would be quarantined. Default = 5

remove { local1 | remote1 }

On the ASR 5000, removes the specified disk from the running RAID causing it to run in degraded mode or to fail.

- **local1** specifies the primary SMC is to be inserted into the RAID.

- **remote1** specifies the backup SMC is to be inserted into the RAID.

remove *hd_num*

On the ASR 5500, removes the specified FSC disk array from the running RAID causing it to run in degraded mode or to fail.

hd_num specifies the RAID is to be established. *hd_num* corresponds to the FSC in slot numbers as shown below:

- hd13 = disk in slot 13
- hd14 = disk in slot 14
- hd15 = disk in slot 15
- hd16 = disk in slot 16
- hd17 = disk in slot 17
- hd18 = disk in slot 18

remove { local1 | local2 }

On the VPC-SI, removes the specified vHD from the running RAID causing it to run in degraded mode or to fail.

- **local1** specifies the primary vHD to be removed from the RAID.
- **local2** specifies the backup vHD to be removed from the RAID.

remove { local1 | remote1 }

On the VPC-DI, removes the specified vHD from the running RAID causing it to run in degraded mode or to fail.

- **local1** specifies the disk on the active Control Function (CF) to be removed from the RAID.
- **remote1** specifies the disk on the backup CF to be removed from the RAID.

select { local1 | remote1 }

On the ASR 5000, selects the specified disk to assemble a RAID when two unrelated RAID disks are present in the system. The resulting RAID runs in degraded mode.

- **local1** specifies the primary SMC is to be inserted into the RAID.
- **remote1** specifies the backup SMC is to be inserted into the RAID.

select { | local1 | local2 }

On VPC-SI, selects the specified vHD to assemble a RAID when two or more unrelated RAID disks are present in the system. The resulting RAID runs in degraded mode.

- **local1** specifies the primary vHD to be inserted into the RAID.

- **local2** specifies the backup vHD to be inserted into the RAID.

select { | local1 | remote1 }

On VPC-DI, selects the specified vHD to assemble a RAID when two or more unrelated RAID disks are present in the system. The resulting RAID runs in degraded mode.

- **local1** specifies the disk on the active Control Function (CF) to be inserted into the RAID.
- **remote1** specifies the disk on the backup CF to be inserted into the RAID.

-noconfirm

Executes the command without displaying "Are you sure" prompt.

-force

Executes the command and overrides warnings.

Usage Guidelines

All commands need confirmation unless the **-noconfirm** is included in the command. If the result will bring down a running RAID, you have to force the command using **-force**.

RAID commands are needed to intervene in the following situations:

- The hard disk controller task can not determine the correct operation.
- Administrative action is required by policy.
- The administrator wants to wipe out an unused disk.

In an automated system, the policies created with this CLI address the possibility of a manually partitioned disk, a disk resulting from a different version of software, a partially constructed disk, or the case of two unrelated disks in the system.

To reduce administrator intervention, a set of policies can be configured to set the default action using the commands in the HD RAID configuration mode. These commands are described in the *HD Storage Policy Configuration Mode Commands* chapter of this guide.

Caution Use of the **hd raid** commands and keywords has the potential for deleting the contents of hard disk drives without the possibility of recovery. You should only use these commands under guidance from the Cisco Technical Assistance Center (TAC).

Important For release 19.2 and higher on the ASR 5500, only those hd<slot> arrays having an FSC in the slot number with available disks can be specified.

Example

The following instructs the system to setup a RAID on the primary ASR 5000 SMC hard drive.

```
hd raid create local1 -force
```

host

Used to resolve the IP address or logical host name information via a DNS query.

Product

x

All

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`host { host_name | host_ip_address }`

host_name | host_ip_address

Specifies the host for which IP information is to be displayed.

host_name: Specifies the logical host name for which the IP address is to be displayed (via DNS lookup). This is an alphanumeric string of 1 through 127 characters.

host_ip_address: Specifies the IP address for which the associated logical host name(s) are to be displayed (via reverse DNS lookup) using IPv4 dotted-decimal notation.

Usage Guidelines

Verify DNS information which affects connections and packet routing.

Example

The following commands will resolve the host information for *remoteABC* and *209.165.200.229* respectively.

```
host remoteABC
host 209.165.200.229
```

install plugin

Unpacks the contents of a patch kit for a specific plugin module. This function is associated with the patch process for accommodating dynamic software upgrades.

Product

ADC

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description **`install plugin`** *`plugin_name patch_file_name`*

plugin_name

Specifies the name of a plugin that has been already copied onto the system as an alphanumeric string of 1 through 16 characters.

patch_file_name

Specifies the file name of the patch (.tgz extension) that was copied onto the system. Ensure that the full file path is copied.

Usage Guidelines Unpacks the contents of a patch kit intended for a specific plugin module. After unpacking the patch you must configure the plugin using the **plugin** command in the Global Configuration mode.

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

Example

To unpack the plugin module named *p2p* with the patch file name *libp2p-1.2.0.tgz* onto the system enter the following command:

```
install plugin p2p libp2p-1.2.0.tgz
```

interface

Configures the system to generate gratuitous ARP (G-ARP) requests in case of a failure during an inter-node online upgrade. If the chassis is not active, an error message displays.

Product All

Privilege Security Administrator, Administrator, Operator, or Inspector with li-administrator permissions

Command Modes Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description **`interface`** *`name`* **`send gratuitous-arp`** *`ip-address`*

Usage Guidelines This command generates a G-ARP for the IP address specified and sends it over the interface.

Example

The following generate a G-ARP for IP address *209.165.200.224.*

```
interface interface_1 send gratuitous-arp 209.165.200.224
```

lawful-intercept

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

lawful-intercept packet-cable

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

lawful-intercept ssdf

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

license

Registers and deregisters the system with Cisco as part of the Cisco Smart Licensing functionality. This command also can be used to manually refresh the Smart Licensing registration information and license information.

Privilege

Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`license smart { deregister | register idtoken` *`id`* **`| renew { auth | id } }`**

deregister

This command contacts the Cisco Smart Software Manager (CSSM) to revoke any previous registration. All Smart Licensing entitlements and certificates on the platform will be removed. All certificates and registration information will be removed from the trusted store. This is true even if the agent is unable to communicate with Cisco to deregister.

If the customer wishes to use Smart Licensing again they will need to run the **license smart register idtoken** command again.

register idtoken *id*

Using the specified ID token the customer received from Cisco Smart Software Manager (CSSM), this command registers this product with Cisco and receives back an identity certificate. This certificate is saved and automatically used for all future communications with Cisco. After registration it will send the current license usage information to Cisco. Every 180 days the agent will automatically renew the registration information with Cisco. The ID token is not saved on the device. By default, the system/product is not registered with the the Cisco Smart Software Manager (CSSM).

id is a string from 1 to 512 characters.

renew { auth | id }

- **auth:** Manually renews authorization of Smart Licenses in use. Since the license authorization is renewed automatically by the system every 6 months, you do not typically need to issue this command.
- **id:** Manually renews the id certificate and registration with CSSM. Since the registration renewal is automatically performed by the system every 6 months, you do not typically need to issue this command.

Usage Guidelines

Before issuing these commands, you must enable Smart Licensing using the **license smart enable** Global Config Mode command.

For additional information, refer to the *Licensing* chapter in the *System Administration Guide*.

Example

To register the system with Cisco Smart Software Manager (CSSM) for Smart Licensing, enter the following command:

```
license smart register
```

link-aggregation port switch to

When a link aggregation group (LAG) contains two sets of ports with each connecting to a different Ethernet switch, this command allows you to change the status of the active distributing ports. (ASR 5x00 only)

Default: none.

Product

All

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

link-aggregation port switch to *slot#* **/** *port#*

slot#

Identifies the physical chassis slot where the line card or MIO card is installed.

port#

Identifies the physical port on the line card or MIO card to automatically switch to.

Usage Guidelines

This command is subject to the following restrictions:

- *slot#/port#* must support LAG.
- *slot#/port#* must be configured with LAG.
- *slot#/port#* must not be actively distributing.

- *slot#/port#* must have negotiated a partner while in standard mode.
- *slot#/port#*'s partner must have a priority equal to or greater than itself.
- *slot#/port#*'s partner bundle must have bandwidth in standard mode equal to or greater than itself.
- Switching to *slot#/port#* must not violate preference within hold-time in standard mode.

Example

```
link-aggregation port switch to 17/2
link-aggregation port switch to 5/12
```

logging active

Enables or disables logging for active internal log files.

Product

All

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
logging active [ copy runtime filters ] [ event-verbosity event_level ] [
pdu-data format ] [ pdu-verbosity pdu_level ]
no logging active
```

no

Indicates the internal logging is to be disabled.

copy runtime filters

Copies the runtime filters and uses that copy to filter the current logging session.

event-verbosity *event_level*

Specifies the level of verboseness to use in logging of events 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.

pdu-data *format*

Specifies output format for packet data units when logged as one of:

- *none*: raw format (unformatted).
- *hex*: hexadecimal format.
- *hex-ascii*: hexadecimal and ASCII similar to a main-frame dump.

pdu-verbosity *pdu_level*

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

Usage Guidelines

Adjust the active logging levels when excessive log file sizes are being generated or, conversely, not enough information is being sent to the active log files for adequate troubleshooting support. The **no** keyword is used to disable internal logging.

Important A maximum of 50,000 events may be stored in each log. Enabling more events for logging may cause the log to be filled in a much shorter time period. This may reduce the effectiveness of the log data as a shorter time period of event data may make troubleshooting more difficult.

Important Once a log has reached the 50,000 event limit the oldest events will be discarded as new log entries are created.

Example

The following sets the active logging for events to the maximum.

```
logging active event-verbosity full
```

The following command sets the active logging for packet data units to level *3* and sets the output format to the main-frame style *hex-ascii*.

```
logging active pdu-data hex-ascii pdu-verbosity 3
```

The following disables internal logging.

```
no logging active
```

logging filter

Sets the logging filtering options for all or individual facilities.

Product All

Privilege Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`logging filter active facility` *`facility`* **`level`** *`severity_level`* **`[ critical-info | no-critical-info ]`**

`logging filter { disable | enable } facility` *`facility`* **`{ all | instance`** *`instance_number`* **`}`**

active

Indicates only active processes are to have logging options set.

disable

Disables logging for a specific instance or all instances. This keyword is only supported for aaamgr, hamgr and sessmgr facilities.

enable

Enables logging for a specific instance or all instances. This keyword is only supported for aaamgr, hamgr and sessmgr facilities.

Important By default logging is enabled for all instances of aaamgr, hamgr and sessmgr.

facility *facility*

Specifies the facility to modify the filtering of logged information. Valid facilities for this command are:

- **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
- **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]
- **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 (Do not use this keyword for HeNB-GW in Release 20, 21.0 and 21.1.)
- **henbgw**: HENB-GW facility (Do not use this keyword for HeNB-GW in Release 20, 21.0 and 21.1.)
- **henbgw-pws**: HENB-GW Public Warning System logging facility (Do not use this keyword for HeNB-GW in Release 20, 21.0 and 21.1.)
- **henbgw-sctp-acs**: HENB-GW access Stream Control Transmission Protocol (SCTP) facility(Do not use this keyword for HeNB-GW in Release 20, 21.0 and 21.1.)
- **henbgw-sctp-nw**: HENBGW network SCTP facility (Do not use this keyword for HNB-GW in Release 20 and later.)
- **henbgwdemux**: HENB-GW Demux facility (Do not use this keyword for HeNB-GW in Release 20, 21.0 and 21.1.)
- **henbgwmgr**: HENB-GW Manager facility (Do not use this keyword for HeNB-GW in Release 20, 21.0 and 21.1.)

- **hnb-gw**: HNB-GW (3G Femto GW) logging facility (Do not use this keyword for HNB-GW in Release 20 and later)
- **hnbmgr**: HNB-GW Demux Manager logging facility (Do not use this keyword for HNB-GW in Release 20 and later)
- **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
- **m3ap**: M3 Application Protocol 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-embms**: MME evolved Multimedia Broadcast Multicast Service 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

all | instance *instance_number*

Specifies whether logging will be disabled or enabled for all instances or a specific instance of aaamgr, hamgr or sessmgr. See additional information in the Usage Guidelines section.

These keywords are only supported for the **disable** and **enable** keywords.

level *severity_level*

This keyword is only supported in conjunction with the **active** keyword.

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

critical-info | no-critical-info

These keywords are only supported in conjunction with the **active** keyword.

critical-info: Specifies that events with a category attribute of critical information are to be displayed. Examples of these types of events can be seen at bootup when system processes and tasks are being initiated. This is the default setting.

no-critical-info: Specifies that events with a category attribute of critical information are not to be displayed.

Usage Guidelines

Apply filters for logged data to collect only that data which is of interest.

To enable logging of a single instance of a facility, you must first disable all instances of the facility (**logging filter disable facility** *facility* **all**) and then enable logging of the specific instance (**logging filter enable facility** *facility* **instance** *instance_number*. To restore default behavior you must re-enable logging of all instances (**logging filter enable facility** *facility* **all**).

Important A maximum of 50,000 events may be stored in each log. Enabling more events for logging may cause the log to be filled in a much shorter time period. This may reduce the effectiveness of the log data as a shorter time period of event data may make troubleshooting more difficult.

Important Once a log has reached the 50,000 event limit the oldest events will be discarded as new log entries are created.

Caution Issuing this command could negatively impact system performance depending on the amount of system activity at the time of execution and/or the type of facility(ies) being logged.

Example

The following are selected examples used to illustrate the various options. Not all facilities will be explicitly shown as each follows the same syntax for options.

The following sets the level to log only *warning* information for *all* facilities.

```
logging filter active facility all level warning
```

The following enables the logging of critical information for the SNMP facility while setting the level to *error*.

```
logging filter active facility snmp level error critical-info
```

The following command disables logging of all aaamgr instances.

```
logging filter disable facility aaamgr all
```

logging trace

Enables or disables the logging of trace information for specific calls, mobiles, or network addresses.

Product

All

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`[ no ] logging trace { callid` *`call_id`* **`| ipaddr`** *`ip_address`* **`| msid`** *`ms_id`* **`| username`** *`user_name`* **`}`**

no

Indicates the logging of trace information is to be disabled.

callid *call_id* | ipaddr *ip_address* | msid *ms_id* | username *user_name*

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

ipaddr *ip_address*: Specifies the IP address in IPv4 dotted-decimal notation for which trace information is to be logged.

msid *ms_id*: Specifies the mobile subscriber ID for which trace information is to be logged as 7 to 16 digits of an IMSI, MIN, or RMI.

username *user_name*: Specifies a previously configured user who is to have trace information logged.

Usage Guidelines

A trace log is useful in troubleshooting subscriber problems as well as for system verification by using a test subscriber. The **no** keyword is used to stop the logging of trace information.

Important A maximum of 50,000 events may be stored in each log. Enabling more events for logging may cause the log to be filled in a much shorter time period. This may reduce the effectiveness of the log data as a shorter time period of event data may make troubleshooting more difficult.

Important Once a log has reached the 50,000 event limit the oldest events will be discarded as new log entries are created.

Caution Issuing this command could negatively impact system performance depending on the number of subscribers connected and the amount of data being passed.

Example

The following commands enables/disables trace information for user *user1*.

```
logging trace username user1
no logging trace username user1
```

The following commands will enable/disable trace information logging for the user assigned IP address *209.165.200.229* .

logging trace ipaddr 209.165.200.229

no logging trace ipaddr 209.165.200.229

The following enables/disables logging of trace information for call ID *fe80AA12*.

logging trace callid fe80AA12

no logging trace callid fe80AA12

logging session fp-flow-state-change

Enables logging for flow offload and onload state change between VPP and sessmgr.

Product

P-GW

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

logging session fp-flow-state-change facility sessmgr instance *instance_number* **number-of-events** *value*

logging session fp-flow-state-change facility sessmgr instance *instance_number* **duration** *value*

[no] logging session fp-flow-state-change facility sessmgr instance *instance number* **number-of-events** *value*

[no] logging session fp-flow-state-change facility sessmgr instance *instance number* **duration** *value*

Event count range is 1–144000, Timer value is 1–120 seconds, and the Integer value is 1-1152.

no

Indicates that the logging information is to be disabled.

facility

Specifies the name of the facility.

all

Specifies all the instances of the facility.

instance

specifies the instance of the facility.

duration

specifies the total duration in seconds to log the events.

number-of-events

Specifies the total number of events to log.

Usage Guidelines

Use this command to enable logging for flow offload and onload state change between VPP and sessmgr. Logs are available on **/hd-raid/fpflowchangelog/fpflowchangelog_** *timestamp*#**.csv**. Example for timestamp is `2021-11-16_05h04m02sEST` since the flow state change logging may have performance impact, this feature must be used with discretion.

Important By default, the monitoring is disabled.

Example

The following command enables logging for flow offload and onload state change between VPP and sessmgr:

```
logging session fp-flow-state-change facility sessmgr instance 8 duration
 10
```

logs checkpoint

Performs checkpointing operations on log data. Checkpointing identifies logged data as previously viewed or marked. Checkpointing results in only the log information since the last checkpoint being displayed; checkpointed log data is not available for viewing.

Individual logs may have up to 50,000 events in the active log. Checkpointing the logs results in at most 50,000 events being in the inactive log files. This gives a maximum of 100,000 events in total which are available for each facility logged.

Product

All

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
logs checkpoint
```

Usage Guidelines

Check point log data to set the log contents to a well-known point prior to special activities taking place. This command may also be a part of periodic regular maintenance to manage log data.

Checkpointing logs moves the current log data to the inactive logs. Only the most recently check pointed data is retained in the inactive logs. A subsequent check pointing of the logs results in the prior check pointed inactive log data being cleared and replaced with the newly check pointed data.

Checkpointing log data marks the active log data to be retained as the inactive log data. This results in the active log data, if displayed, having no data earlier than the point in time when the checkpointing occurred.

Important Checkpointing logs should be done periodically to prevent the log files becoming full. Logs which have 50,000 events logged will discard the oldest events first as new events are logged.

Important An Inspector-level administrative user cannot execute this command.

Example

The following command immediately sets a checkpoint for event logs and moves the current log data to inactive logs:

```
logs checkpoint
```

lsp-ping

Checks Multi Protocol Label Switching (MPLS) label switch path (LSP) connectivity for the specified IPv4 forwarding equivalence class (FEC). It must be followed by an IPv4 FEC prefix.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description **`lsp-ping`** *`ip_prefix_FEC`* **`[ count`** *`ping_packets`* **`] [ | verbose ] [ | grep`** *`grep_options`* **`]`**

ip_prefix_FEC

Specifies an IP prefix FEC with or without subnet mask entered using IPv4 dotted-decimal CIDR notation.

count *ping_packets*

Sets the number of ping packets to be sent as an integer from 1 through 16. Default: 4.

Important The timeout interval for the packets is 5 seconds by default.

verbose

Sets the verbose (detailed) output mode.

grep*grep_options*

Pipes (sends) the output of this command to the **grep** command.

Usage Guidelines This command is used to verify the MPLS LSP connectivity for the specified FEC.

Example

Following are the examples for using this command with all possible options for IPv4 address *209.165.200.225* and mask *32* (CIDR notation):

```
lsp-ping 209.165.200.225/32
lsp-ping 209.165.200.225/32 count 15
lsp-ping 209.165.200.225/32 verbose
```

lsp-traceroute

Discovers MPLS LSP routes that packets actually take when traveling to their destinations. It must be followed by an IPv4 or IPv6 FEC prefix.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description **lsp-traceroute** *ip_prefix_FEC* **[maxttl** *time_to_live* **] [| verbose] [| grep** *grep_options* **]**

ip_prefix_FEC

Specifies the destination IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal with or without mask (CIDR notation).

maxttl *time_to_live*

Sets the maximum time to live in hops. TTL is an integer from 1 through 255. Default: 30.

verbose

Sets the verbose (detailed) output mode.

grep*grep_options*

Pipes (sends) the output of this command to the **grep** command.

Usage Guidelines This command is used or the router to discover the MPLS LSP routes through which the packets will travel to their IPv4 or IPv6 destinations.

Example

The following command specifies the destination IP address *209.165.200.237* for which the MPLS routes will be discovered for packets to traverse:

```
lsp-traceroute 209.165.200.237/32
```

mkdir

Creates a new directory in the local file system or in remote locations as specified.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description **mkdir** *filepath*

filepath

Specifies the directory path to create. The path must be formatted as follows:

For the ASR 5000:

[file:]{ /flash | /pcmcia1 | /hd-raid }[/*directory* **]/***file_name*

Important Use of the ASR 5000 SMC hard drive is not supported in this release.

For the ASR 5500:

[file:]{ /flash | /usb1 | /hd-raid }[/*directory* **]/***file_name*

For VPC:

[file:]{ /flash | /hd-raid | /usb1 | /usb2 | /cdrom1 }[/*directory* **]/***file_name*

Important The USB ports and CDROM must be configured via the hypervisor to be accessible.

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

Usage Guidelines Create new directories as part of periodic maintenance activities to better organize stored files.

Example

The following creates the directory */flash/pub* in the local flash storage.

```
mkdir /flash/pub
```

mme-mmedemux

Configures the MME Manager related commands.

Product MME

Privilege Security Administrator, Administrator

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description **`mme mmedemux { audit-with | s1ap-sync } mmemgr { all | instance`** *`value`* **`}`**

mme

Configures the MME exec commands.

mmedemux

Configures the MME Manager related commands.

audit-with

Performs audit with MME Manager.

s1ap-sync

Synchronizes with s1ap association count with MME Manager-Archive with all instances of MME Manager.

mmemgr

Synchronizes up with MME Manager on eNodeB list.

all

Synchronizes up with MME Manager on eNodeB list with all instances.

instance *value*

Synchronizes with MME Manager on eNodeB list with specific instance. *value* Must be an integer from 1 to 48.

mme disconnect

Performs a graceful/ungraceful disconnection of an SCTP peer.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

mme disconnect { s1-peer *peer_ID* **[graceful] [-noconfirm] | sgs-peer** *peer_ID* **[-noconfirm | perform-imsi-detach [-noconfirm | detach-rate** *detach_rate* **[-noconfirm]]] }**

s1-peer *peer-ID*

Specifies the eNodeB peer ID which has to be disconnected. *peer-ID* is an integer from 1 through 4294967295.

graceful

Specifies that the SCTP connection to the S1 peer will be terminated with a complete handshake. By default (without this keyword), SCTP connections are aborted.

sgs-peer *peer-ID*

Specifies the SGs peer ID which has to be disconnected. *peer-ID* must be an integer from 1 through 4294967295.

perform-imsi-detach

Performs IMSI detach.

detach-rate *detach-rate*

Detaches per cycle. . *detach-rate* must be an integer from 1 to 100.

-noconfirm

Executes the command without any additional prompts or confirmation from the user.

Usage Guidelines

Use this command to disconnect the SCTP connection to the specified peer eNodeB. This command can be used to remove stale eNodeB connections from the MME, even when no active SCTP connection exists.

Example

The following gracefully disconnects the SCTP connection with the eNodeB with a peer ID of 22315734:

```
mme disconnect s1-peer 22315734 graceful -noconfirm
```

mme imsimgr

Triggers an MME IMSIMgr audit for IMSI, IMEI, MSISDN information for a specific SessMgr instance associated with a specific IMSIMgr instance.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`mme imsimgr instance` *`instance_id`* **`audit-with sessmgr { all | instance`** *`instance_id`* **`}`**

imsimgr instance *instance_id*

Specifies the IMSI manager instance for which the audit is initiated. The audit is initiated for only one specified instance of IMSI manager at a time.

instance_id : Enter an integer from 1 through 4.

audit-with sessmgr { all | instance *instance_id* }

Initiates an IMSIMgr for either all associated session managers or for a specific session manager (SessMgr) instance.

all | instance *instance_id*: Select **all** to initiate the audit for all SessMgr instances or select **instance** and for *instance_id* enter an integer from 1 to 1152 to identify a specific SessMgr for the audit.

Usage Guidelines

Use this command to manage the IMSIMgr's IMSI table, and to initiate an audit of one or more SessMgrs associated with the specific IMSIMgr. This is useful when the MME has been configured to support more than one MME IMSIMgr. The audit assists you to ensure that the IMSI table has the correct IMSI-SessMgr association.triggers as the audit checks for IMSI, IMEI, MSISDN information for a specific SessMgr instance.

Example

Use a command similar to the following to trigger an audit of SessMgr 243 associated with IMSIMgr 2:

```
mme imsimgr instance 2 audit-with sessmgr instance 243
```

mme offload

Initiates or stops the offload of UEs associated with a specified MME service.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

The following command syntax is available in Release 12.2 and earlier.

```
mme offload mme-service mme_svc_name { start mme-init-release-timeout seconds
 paging-init-timeout seconds | stop }
```

The following command syntax is available in Release 14.0 and higher.

```
mme offload mme-service mme_svc_name { time-duration minutes offload-percentage
 percent [ disable-implicit-detach | preserve-volte-subscribers  ] ] | stop
 } [- noconfirm ]
```

mme-service *name*

Specifies the name of an existing MME service from which UEs will be offloaded as an alphanumeric string of 1 trough 63 characters.

start mme-init-release-timeout *seconds* paging-init-timeout *seconds*

These keywords are available in Release 12.2 and earlier.

Sets the timeout for the initial release procedure and the paging procedure.

start mme-init-release-timeout *seconds*: Configures the timeout (in seconds) for triggering the IDLE MODE ENTRY procedure for UEs that are in the ECM_CONNECTED state as an integer from 1 to 120. The cause of the IDLE MODE ENTRY will be "Load balancing TAU required".

paging-init-timeout *seconds*: Configures the timeout (in seconds) for triggering the PAGING procedure for UEs in the ECM_IDLE state as an integer from 1 to 120. After returning the UEs to the ECM_CONNECTED state, the IDLE MODE ENTRY procedure is triggered with the "Load balancing TAU required" cause.

time-duration *minutes* offload-percentage *percent*

time-duration specifies the maximum allowed time for the UE offload procedure to complete.

minutes can be any value 1 through 1000 minutes.

offload-percentage specifies the percentage of total subscribers on this mme-service to offload.

percent can be any value 0 through 100.

disable-implicit-detach

By default, if the UE context is not transferred to another MME within 5 minutes, the UE will be implicitly detached. This option disables this implicit detach timer.

stop

Ends the offload process.

-noconfirm

Executes the command without any additional prompts or confirmation from the user.

preserve-volte-subscribers

This keyword is used to configure preservation of VoLTE subscribers from offloading during active calls (QCI=1). By default, the subscribers with voice bearer with QCI = 1 will not be preserved during MME offloading. Configuring the keyword **preserve-volte-subscribers** enables preservation of subscribers with voice bearer.

Usage Guidelines

Use this command to initiate or stop the offloading of UEs associated with a specified MME service.

Prior to initiating this command, you can set the **relative-capacity** command in the MME Service Configuration Mode to zero (0). This prevents this MME from accepting any new calls, and redirects them to other MMEs in the pool while existing UEs on this MME are removed.

Important Emergency attached UEs in Connected or Idle mode are not considered for offloading.

Example

This example applies to Release 12.2 and earlier.

The following command sets the trigger to start off-loading UEs from a service named *mme3* at *60* seconds and the paging trigger at *90* seconds:

```
mme offload mme-service mme3 start mme-init-release-timeout 60
paging-init-timeout 90
```

Example

This example applies to Release 14.0 and higher.

The following example command rebalances (offloads) 30 percent of all UEs from the specified mme-service (to other mme-services in the MME pool) over the course of 10 minutes.

```
mme offload mme-service mme_svc time-duration 10 offload-percentage 30
-noconfirm
```

Example

The following example command re-balances(offloads) 30 percent of Non-VoLTE subscribers from the specified mme-service (to other mme-services in the MME pool) over the course of 30 minutes with VoLTE preservation.

```
mme offload mme-service mmesvc  time-duration 30 offload-percentage 30
preserve-volte-subscribers
```

mme paging cache clear

Enables the operator to clear the paging cache for either a specific SessMgr instance or for all SessMgrs.

Product

MME.

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
mme paging cache clear { all | instance  sessmgr_instance }
```

all

Instructs the MME to clear the paging cache for all Session Managers.

instance *sessmgr_instance*

Enter an integer from 0 to 4294967295 to specify a single Session Manager.

Usage Guidelines

This command clears the cache. It is important to clear the cache after the **mme paging cache size** is set to zero (0) to stop caching. This clear command needs to be used to reset the cache after caching is stopped.

Example

Use the following command to clear the paging cache for all SessMgrs:

```
mme paging cache clear  all
```

mme relocate-ue imsi

This command enables the operator to detach a UE from the current MME and cause it to reattach to another MME in the pool.

Product MME

Privilege Security Administrator, Administrator

Command Modes Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description **mme relocate-ue imsi** *imsi* **new-guti mme-group-id** *grp_id* **mme-code** *mme_code* **m-tmsi** *mtmsi*

imsi *imsi*

Specifies the Mobile Station Identifier of the UE to be relocated. This UE must be registered or connected to this MME.

new-guti mme-group-id *group_id*

The group to which the target MME belongs.

grp_id :

- Beginning with Releases 16.5, 17.4, and 18.2 and forward, the valid range for mme group id is an integer from 0 through 65536.
- Previous releases, the valid range for mme group id is an integer from 32768 through 65536.

mme-code *mme_code*

The target MME to which this UE should be attached.

mme_code : The unique identifier for the target MME; must be an integer from 0 through 255.

m-tmsi *mtmsi*

The new GUTI MME-TMSI for this UE.

mtmsi : An integer from 0 through 4294967295.

Usage Guidelines MME uses this configuration to relocate UEs to a different MME using IMSI, mme-group-id, mme-code and m-tmsi.

mme reset

Sends an S1 RESET message to a designated eNodeB to reset all UE-associated S1 connections.

Product MME

Privilege Security Administrator, Administrator

Command Modes Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`mme reset s1-peer` *`peer_ID`*

s1-peer *peer-ID*

Specifies an existing eNodeB peer ID to which the REST message is to be sent as an integer from 1 through 4294967295.

Usage Guidelines

Use this command to send an S1 RESET message to a designated eNodeB to reset all UE-associated S1 connections.

The S1 peer ID for an eNodeB can be identified by executing the **show mme-service enodeb-association** command available in this mode. The peer ID is presented in the "Peerid" field.

Example

The following command initiates the sending of an S1-peer reset message to an eNodeB with a peer ID of *22315734*:

```
mme reset s1-peer 22315734
```

monitor interface

Enables monitoring of traffic on a particular interface.

Product

All

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`monitor interface` *`if_name`*

if_name

Specifies the name of the interface to be monitored as an alphanumeric string of 1 through 79 characters.

Usage Guidelines

Use this command to monitor the traffic on a specified interface.

Example

This command monitors the traffic on the interface named *if1001*:

```
monitor interface if1001
```

monitor protocol

Enters the system's protocol monitoring utility.

Product

All

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`monitor protocol`

Usage Guidelines

Useful for troubleshooting, this command provides a tool for monitoring protocol transactions between the system and other network nodes including the mobile station(s).

The following protocols can be monitored:

- SNMP
- RADIUS Authentication
- RADIUS Accounting
- A11 (R-P Interface) (PDSN only)
- Mobile IPv4
- A11MGR
- PPP
- A10
- User L3 (User Layer 3 protocols)
- USERTCP STACK
- L2TP
- L2TPMGR
- L2TP Data
- GTPC
- GTPCMGR
- GTPU
- GTPP

Important If the hard disk drive (HDD) is used for CDR storage, the CDR option must be used and not the GTPP option (27).

- DHCP (GGSN only)
- CDR
- DHCPV6
- RADIUS COA
- MIP Tunnel
- L3 Tunnel (Layer 3 Tunnel Protocols)
- CSS Data
- CSS Signaling

Important In StarOS 9.0 and later releases the CSS Data Signaling option is not supported.

- EC Diameter (Diameter Enhanced Charging)
- SIP (IMS)
- IPSec IKE Inter-Node
- IPSec IKE Subscriber
- IPSG RADIUS Signal
- ROHC (Robust Header Compression)
- WiMAX R6
- WiMAX Data
- SRP
- BCMCS SERV AUTH
- RSVP
- Mobile IPv6
- ASNGWMGR
- STUN
- SCTP: Enabling this option will display the SCTP protocol message packets on HNB-GW node.

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- M3UA
- SCCP
- TCAP
- MAP
- RANAP
- GMM
- GPRS-NS
- BSSGP
- CAP
- SSCOP
- SSCFNNI
- MTP3
- LLC
- SNDCP
- BSSAP+
- SMS
- PHS-Control (Payload Header Compression)
- PHS-Data
- DNS Client
- MTP2
- HNBAP: Enabling this option will display the HNB Application Part (HNBAP) protocol packets.

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- RUA: Enabling this option will display the RANAP User Adaptation (RUA) protocol packets.
- EGTPC
- App Specific Diameter: Enabling this option will display the following sub-options —
  - 1 - DIABASE (OFF)
  - 2 - DIAMETER Gy (OFF)
  - 3 - DIAMETER Gx/Ty/Gxx (OFF)
  - 4 - DIAMETER Gq/Rx/Tx (OFF)
  - 5 - DIAMETER Cx (OFF)

- 6 - DIAMETER Sh (OFF)
- 7 - DIAMETER Rf (OFF)
- 8 - DIAMETER EAP/STa/S6a/S6d/S6b/S13/SWm (OFF)
- 9 - DIAMETER HDD (OFF)

- PHS-EAPOL
- ICAP
- Micro-Tunnel
- ALCAP: Enabling this option will display the Access Link Control Application Part (ALCAP) protocol message packets on HNB-GW node.

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- SSL
- S1-AP
- NAS
- LDAP
- SGS
- AAL2: Enabling this option will display the ATM Adaptation Layer 2 (AAL2) protocol message packets on HNB-GW node.

Important In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

- PHS (Payload Header Suppression)
- PPPOE
- RTP (IMS)
- RTCP (IMS)
- LMI
- NPDB (IMS)
- SABP (Femto-UMTS)
- OCSP (X.509)

Once the protocol has been selected by entering its associated number, the utility monitors and displays every relative protocol message transaction.

Protocol monitoring is performed on a context-by-context-basis. Therefore, the messages displayed are only those that are transmitted/received within the system context from which the utility was executed.

For additional information on using the monitor utility, refer to the *System Administration Guide*.

Caution Protocol monitoring can be intrusive to subscriber sessions and could impact system performance. Therefore, it should only be used as a troubleshooting tool.

Example

The following command opens the protocol monitoring utility for SIP (IMS) = *37*:

```
monitor protocol 37
```

monitor subscriber

Enables the system's subscriber monitoring utility. Available keywords vary based on the licenses installed on the system.

Product

All

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

monitor subscriber [asn-peer-address *bs_peer_address* **| callid** *call_id* **fng-peer-address** *ipv4_address* **| global-enb-id** *global-enb-id* **| imei** *imei_value* **| imsi** *imsi_value* **| ipaddr** *ip_address* **| ipv6addr** *ipv6_address* **| ipsg-peer-address** *ipsg_peer_address* **| msid** *ms_id* **| msisdn** *msisdn* **| next-call | pcf** *pcf_address* **| pdif-peer-address** *pdif_peer_address* **| peer-fa** *peer_fa_address* **| peer-lac** *lac_peer_address* **| sgsn-address** *sgsn_address* **| type { 1xrtt | asngw | asnpc | closedrp | evdorev0 | evdoreva | interrogating-cscf | ggsn [Next-Call By APN] | ha | ipsg | lns | mme | pdif | proxy-cscf | rfc3261-proxy | serving-cscf } next-call | type bcmcs { next-call | next-service-request } | username** *user_name* **| Next-Call By APN]**

asn-peer-address *bs_peer_address*

Specifies the peer ASN Base Station IP address in IPv4 address in dotted-decimal notation.

callid *call_id*

Specifies the call identification number assigned to the subscriber session by the system to be monitored as a 4-byte hexadecimal number.

fng-peer-address *ipv4_address*

Specifies the specific FNG WLAN IP address in IPv4 dotted-decimal notation.

global-enb-id *global-enb-id*

Specifies the Global eNodeB ID. This must be followed by MCC-MNC-eNBType-eNBID.

MCC consists of 3 digits.

MNC consists of 2 or 3 digits.

eNBType is 0 for Macro and 1 for Home.

eNBID has max 1048575 for MACRO eNB and max 268435456 for Home eNB.

imei *imei_value*

International Mobile Equipment Identification (IMEI). Must be followed by 8 digits of TAC (Type Allocation Code) and 6 digits of SNR (Serial Number). Only the first 14 digit of IMEI/IMEISV is used to find the equipment ID.

imsi *imsi_value*

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

ipaddr *ip_address*

Specifies the IP address of the subscriber session to be monitored in IPv4 dotted-decimal notation.

ipv6addr *ipv6_address*

Specifies the IPv6 address of the subscriber session to be monitored in IPv6 colon-separated-hexadecimal notation.

ipsg-peer-address *ipsg_peer_address*

Specifies the peer IPSG IP address. Must be followed by an IPv4 address in dotted -decimal notation.

msid *ms_id*

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

msisdn *msisdn*

Specifies the Mobile Subscriber ISDN number to be monitored as 7 to 16 digits of an IMSI, MIN, or RMI.

next-call

Specifies that the system will monitor the next incoming subscriber session.

Entering this keyword will display the available options of protocols to select. For a list of supported protocols with this keyword, refer to the **monitor protocol** command.

pcf *pcf_address*

Specifies the PCF IP address in IPv4 dotted-decimal notation.

pdif-peer-address *pdif_peer_address*

Specifies the peer PDIF IP address in IPV4 dotted-decimal notation.

peer-fa *peer_fa_address*

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

peer-lac *lac_peer_address*

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

sgsn-address *sgsn_address*

Specifies the SGSN IP address in IPv4 dotted-decimal notation.

type { 1xrtt | asngw | asnpc | bcmcs { next-call | next-service-request } closedrp | evdorev0 | evdoreva | | fng | interrogating-cscf | ggsn [Next-Call By APN] | ha | ipsg | lns | mme | openrp | pdif | pgw | proxy-cscf | rfc3261-proxy | saegw | serving-cscf } next-call [apn *apn*]

Allows monitoring for specific subscriber types established in the system when next call occurs.

- **1xrtt**: Displays logs for cdma2000 1xRTT call session subscriber
- **asngw**: Displays logs for ASN-GW call session subscriber
- **asnpc**: Displays logs for ASN PC/LR call session subscriber
- **bcmcs**: Displays logs for Broadcast and Multicast Service
- **closedrp**: Displays logs for cdma2000 Closed-RP call session subscriber
- **evdorev0**: Displays logs for cdma2000 EVDO Rev0 call session subscriber
- **evdoreva**: Displays logs for cdma2000 EVDO RevA call session subscriber
- **fng**: Displays logs for the FNG session subscriber
- **interrogating-cscf**: Displays logs for Interrogating CSCF subscriber
- **ggsn**: Displays logs for UMTS GGSN call session subscriber
- **Next-Call By APN**: Display logs for next call on APN basis, where APN name can be any Gi or Gn APN.
- **ha**: Displays logs for Home Agent call session subscriber
- **ipsg**: Displays logs for IPSG call session subscriber
- **lns**: Displays logs for LNS call session subscriber
- **mme**: Displays logs for MME session subscribers.
- **openrp**: Displays logs for OpenRP subscriber

- **pgw**: Displays logs for P-GW call session subscriber
- **pdif**: Displays logs for PDIF call session subscriber
- **proxy-cscf**: Displays logs for Proxy CSCF subscriber
- **rfc3261-proxy-cscf**: Displays logs for non-ims-proxy (RFC-3261 proxy) subscriber
- **saegw**: Displays logs for SAEGW call session subscriber
- **serving-cscf**: Displays logs for Serving CSCF subscriber

username *user_name*

Specifies the username of an existing subscriber to be monitored.

Usage Guidelines

The monitor subscriber utility provides a useful tool for monitoring information about and the activity of either a single subscriber or all subscribers with active sessions within a given context.

Caution The **monitor subscriber** command is intended for *system debugging only.* This command is complementary to external tracing systems and not meant as a replacement for ongoing external system monitoring.

The following items can be monitored:

- Control events
- Data events
- Event ID information
- Inbound events
- Outbound events
- Protocols (identical to those monitored by command)

Once the criteria has been selected, the utility will monitor and display every relative piece of information on the subscriber(s).

For additional information on using the monitor utility, refer to the *System Administration Guide*.

Important Option Y for performing multi-call traces is only supported for use with the GGSN. This option is available when monitoring is performed using the "Next-Call" option. It allows you monitor up to 11 primary PDP contexts for a single subscriber.

Subscriber monitoring is performed on a context-by-context-basis. Therefore, the information displayed will be only that which is collected within the system context from which the utility was executed.

Caution Subscriber monitoring can be intrusive to subscriber sessions and could impact system performance; therefore, it should only be used as a troubleshooting tool.

Example

The following command enables monitoring for user *user1*.

monitor subscriber username user1

The following command will enable monitoring for the user assigned IP address *209.165.200.229*.

monitor subscriber ip-address 209.165.200.229

The following enables monitoring for call ID *FE80AA12*.

monitor subscriber callid fe80aa12

newcall policy

Configures new call policies for busy-out conditions.

Product

ASN-GW

ASN PC/LR

ePDG

GGSN

HA

HNB-GW

IPCF

LNS

MME

PDSN

P-GW

S-GW

SAEGW

SaMOG

SGSN

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

newcall policy { asngw-service | asnpc-service | ePDG-service | sgsn-service } { all | name *service_name* **} reject**

newcall policy { fa-service | lma-service | lns-service | mipv6ha-service } { all | name *service_name* **} reject**
newcall policy ggsn-service { apn name *apn_name* **| all | name** *service_name* **} reject [release-existing-session]**
newcall policy { ha-service | pdsn-service | pdsnclosedrp-service } { all | name *service_name* **} { redirect** *target_ip_address* **[weight** *weight_num* **] [** *target_ipaddress2* **[weight** *weight_num* **] ... target_ip_address16 [weight** *weight_num* **] | reject }**
newcall policy hnbgw-service { all | name *service_name* **} reject**
newcall policy mme-service { all | name *service_name* **} reject**
newcall policy { pcc-af-service | pcc-policy-service } { all | name *service_name* **} reject**
newcall policy pgw-service { all | apn name *apn_name* **| name** *service_name* **} reject [release-existing-session]**
newcall policy saegw-service { all | name *service_name* **} reject [release-existing-session]**
newcall policy sgw-service { all | name *service_name* **} reject [release-existing-session]**
newcall policy samog-service { all | name *service_name* **} drop**

no newcall policy { asngw-service | asnpc-service | epDG-Service } { all | name *service_name* **}**
no newcall policy { fa-service | ggsn-service | ha-service | lma-service | lns-service | mipv6ha-service | pdsn-service| pdsnclosedrp-service } { all | name *service_name* **}**
no newcall policy ggsn-service { apn *apn_name* **| all | name** *service_name* **}**
no newcall policy { ha-service | pdsn-service } { all | name *service_name* **} redirect** *target_ip_address* **[weight***weight_num* **] [** *target_ip_address2* **[weight** *weight_num* **] ... target_ip_address16 [weight***weight_num* **]**
no newcall policy hnbgw-service { all | name *service_name* **}**
no newcall policy mme-service { all | name *service_name* **}**
no newcall policy { pcc-af-service | pcc-policy-service } { all | name *service_name* **}**
no newcall policy pgw-service { all | apn name *apn_name* **| name** *service_name* **}**
no newcall policy saegw-service { all | name *service_name* **}**
no newcall policy sgw-service { all | name *service_name* **}**
no newcall policy samog-service { all | name *service_name* **}**

no

Disables the new call policy for all or specified service of a service type.

no newcall policy { ha-service | pdsn-service } { all | name ***service_name*** **} redirect** ***target_ip_address*** **[weight** ***weight_num*** **] [** ***target_ip_address2*** **[weight** ***weight_num*** **] ... *target_ip_address16* [weight** ***weight_num*** **]**

Deletes up to 16 IP addresses from the redirect policy. The IP addresses must be expressed in IPv4 dotted-decimal notation

newcall policy { asngw-service | asnpc-service | epDG-service }{ all | name *service_name* } reject

Creates a new call policy to reject the calls based on the specified ASN-GW or ASN PC/LR service name or all services of this type.

asngw-service: Specifies the type of service as ASN GW for which new call policy is configured.

asnpc-service: Specifies the type of service as ASN PC/LR for which new call policy is configured.

epDG-service: Specifies the type of service as ePDG for which new call policy is configured.

name *service_name*: Specifies the name of the service for which new call policy is configured. service_name is name of a configured ASN GW or ASN PC/LR service.

reject: Specifies that the policy rejects new incoming calls. Depending on the type of service that the policy is applied to, the reason codes are reported as part of the reply to indicate the rejection. For ASN-GW and ASN PC/LR service rejection code is 81H (Registration Denied - administratively prohibited).

Note When the newcall policy reject CLI command is enabled, S-GW allows new subscribers with Emergency-APN trying to attach a new session request and have uniform Emergency APN support is available across different modes for S-GW and P-GW (SGW+PGW, Colocated SAEGW).

newcall policy { fa-service | lma-service | lns-service | mipv6ha-service }{ all | name *service_name* } reject

Creates a new call policy that rejects calls based on the specified access point name.

fa-service | ha-service | lma-service | lns-service | mipv6ha-service | mme-service | pdsn-service | pdsnclosedrp-service

Specifies the type of service for which to configure a new call policy. The following services are supported:

- **fa-service**: A Foreign Agent service
- **ha-service**: A Home Agent service
- **lma-service**: A Local Mobility Anchor (LMA) service
- **lns-service**: An L2TP Network Server service
- **mipv6ha-service**: A Mobile IPv6 Home Agent service
- **pdsn-service**: A Packet Data Serving Node service
- **pdsnclosedrp-service**: A Closed R-P service

{ all | name *service_name* }

Specifies a filter for the new call policy. Whether the new call policy will be applied to all configured services or a specific one.

- **all**: Specifies that the new call policy will be applied to all instances of the selected service type.
- **name**: *service_name*: Specifies the name of a specific instance of the selected service type as an alphanumeric string of 1 through 63 characters that is case sensitive.

redirect *target_ip_address* [weight *weight_num*] [*target_ip_address2* [weight *weight_num*] ... *target_ip_address16* [weight *weight_num*]

Configures the busy-out action. When a redirect policy is invoked, the service rejects new sessions and provides the IP address of an alternate destination. This command can be issued multiple times.

target_ip_address# is the IP address of an alternate destination expressed in IPv4 dotted-decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values.

weight *weight_num*: When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified the entry is automatically assigned a weight of 1. *weight_num* must be an integer from 1 through 10.

Depending on the type of service that the policy is applied to, the following reason codes are reported as part of the reply:

- **ha service:** 88H (Registration Denied - unknown home agent address)
- **pdsn service:** 88H (Registration Denied - unknown PDSN address)

Important The redirect option is not supported for use with FA and GGSN services.

reject

Specifies that the policy rejects new incoming calls. Depending on the type of service that the policy is applied to, the following reason codes are reported as part of the reply to indicate the rejection:

- **asngw service**: 81H (Registration Denied - administratively prohibited)
- **fa service:** 41H (administratively prohibited)

Important When **newcall policy** is set to reject for the FA service, the Busy Bit is set in the Agent Advertisement. Any further RRQs will be rejected with this code value.

- **ggsn service:** C7H (Rejected - no resources available)
- **ha service:** 81H (Registration Denied - administratively prohibited)
- **mipv6ha-service**: 81H (Registration Denied - administratively prohibited)
- **mme service:** 81H (Registration Denied - administratively prohibited)
- **pdsn service:** 81H (Registration Denied - administratively prohibited)
- **pdsnclosedrp-service**: 81H (Registration Denied - administratively prohibited)

newcall policy hnbgw-service { all | name *service_name* } reject

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.

Creates a new call policy to reject the calls in a specified HNB-GW service name instance or all HNB-GW services on the system.

name *service_name*: Specifies the name of the HNB-GW service for which new call policy is configured.

reject: Specifies that the policy rejects all new incoming calls. Depending on the type of service that the policy is applied to, the reason codes are reported as part of the reply to indicate the rejection. For HNB-GW service rejection code is 81H (Registration Denied - administratively prohibited).

newcall policy mme-service { all | name *service_name* } reject

Creates a new call policy to reject the calls based on the specified MME service name or all MME services on the system.

name *service_name*: Specifies the name of the MME service for which new call policy is configured.

reject: Specifies that the policy rejects new incoming calls. Depending on the type of service that the policy is applied to, the reason codes are reported as part of the reply to indicate the rejection. For MME service rejection code is 0x16 (Registration Denied - administratively prohibited).

newcall policy { pcc-af-service | pcc-policy-service | pcc-quota-service} { all | name *service_name* } reject

Creates a new call policy to reject the calls for PCC services on the system for any of the following PCC services:

- **pcc-af-service name** *service_name*: Specifies the Policy and Charging Control-Application Function (PCC-AF) service for which new call policy is to be configured on the system.

  name *service_name*: Specifies the name of an existing PCC-AF service for which new call policy is configured.

- **pcc-policy-service name** *service_name*: Specifies the Policy and Charging Control-Policy (PCC-Policy) service for which new call policy is to be configure on the system.

  name *service_name*: Specifies the name of an existing PCC-Policy service for which new call policy is configured.

reject: Specifies that the policy rejects new incoming calls. Depending on the type of service that the policy is applied to, the reason codes are reported as part of the reply to indicate the rejection. For PCC services rejection code is 81H (Registration Denied - administratively prohibited).

newcall policy pgw-service { all | apn name *apn_name* | name *service_name* } reject [release-existing-session]

Creates a new call policy to reject the calls based on the specified P-GW service name, APN name, or all P-GW services (and any SAEGW service associated with the P-GW service) in this context .

all: Rejects all P-GW services on the system. Specifies that the new call policy will be applied to all instances of the P-GW service, and any associated SAEGW service, in this context.

apn *apn_name*: Specifies the name of the APN, and any associated P-GW/SAEGW service, for which new call policy is configured.

name *service_name*: Specifies the name of the P-GW service, and any SAEGW service associated with this P-GW service, for which new call policy is configured.

reject: Specifies that the policy rejects new incoming calls. Depending on the type of service that the policy is applied to, the reason codes are reported as part of the reply to indicate the rejection.

release-existing-session: All the pre-existing sessions across all eGTP/GTP services for that IMSI/IMEI will be released gracefully. Without this keyword, the receiving node rejects the CSReq without considering the existing sessions for that IMSI/IMEI, which may lead to junk sessions. Disabled by default.

newcall policy saegw-service { all | name *service_name* } reject [release-existing-session]

Creates a new call policy to reject the calls based on the specified SAEGW service name or all SAEGW services on the system.

name *service_name*: Specifies the name of the SAEGW service for which new call policy is configured.

reject: Specifies that the policy rejects new incoming calls. Depending on the type of service that the policy is applied to, the reason codes are reported as part of the reply to indicate the rejection.

Important When **newcall policy saegw-service all reject** CLI command is enabled, the handovers incoming to the S-GW part of an SAEGW, and any other applicable handovers, are not rejected.

release-existing-session: All the pre-existing sessions across all eGTP/GTP services for that IMSI/IMEI will be released gracefully. Without this keyword, the receiving node rejects the CSReq without considering the existing sessions for that IMSI/IMEI, which may lead to junk sessions. Disabled by default.

newcall policy sgw-service { all | name *service_name* } reject [release-existing-session]

Creates a new call policy to reject the calls based on the specified S-GW service name or all S-GW services on the system.

name *service_name*: Specifies the name of the S-GW service for which new call policy is configured.

reject: Specifies that the policy rejects new incoming calls. Depending on the type of service that the policy is applied to, the reason codes are reported as part of the reply to indicate the rejection.

release-existing-session: All the pre-existing sessions across all eGTP/GTP services for that IMSI/IMEI will be released gracefully. Without this keyword, the receiving node rejects the CSReq without considering the existing sessions for that IMSI/IMEI, which may lead to junk sessions. Disabled by default.

newcall policy samog-service { all | name *service_name* } drop

Creates a new call policy to drop calls based on the specified SaMOG service name or all SaMOG services on the system. By default, this configuration is disabled.

name *service_name*: Specifies the name of the SaMOG service for which new call policy is configured. *service_name* must be an alphanumeric string of 1 through 63 characters.

drop: Specifies the policy to drop new incoming calls. When the retries are exhausted, the AP/WLC attempt session creation on alternate SaMOG services connected to the AP/WLC.

Usage Guidelines This command is used to busy-out specific system services prior to planned maintenance or for troubleshooting. This is required when operator find out that the system is somehow overloaded, or needs some kind of maintenances or so.

Example

The following command creates a new call policy to re-direct all new calls for all PDSN services to a device having an IP address of *209.165.200.224*:

```
newcall policy pdsn-service all redirect 209.165.200.224
```

The following command creates a new call policy to reject all new calls for a GGSN service called *ggsn1*:

```
newcall policy ggsn-service name ggsn1 reject
```

The following command creates a new call policy to reject all new calls for an MME service called *MME1*:

```
newcall policy mme-service name MME1 reject
```

The following command creates a new call policy to reject all new calls for an HNB-GW service called *hnbgw1*:

```
newcall policy hnbgw-service name hnbgw1 reject
```

The following command creates a new call policy to reject all new calls for a PCC Policy service called *pcrf1*:

```
newcall policy pcc-policy-service name pcrf1 reject
```

The following command creates a new call policy to drop all new calls for the SaMOG service:

```
newcall policy samog-service all drop
```

password change

Provides a mechanism for local-user administrative users to change their passwords.

Product All

Privilege All local-user administrative levels except as noted below

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description **password change [local-user** *name* **]**

local-user *name*

Specifies the name of an existing local-user administrative user for which to change the password as an alphanumeric string of 3 through 144 characters that is case sensitive.

Important This keyword is only available to local-users with an authorization level of security-administrator.

Usage Guidelines

This command provides a mechanism for local-user administrative users to change their passwords. In addition, it also provides a mechanism for security-administrator local-users to change the password for other local-user accounts.

If the **local-user** keyword is not entered, the system prompts the user for their current password and for the new password. New passwords take effect at the next login. Users that have had their password changed by a security-administrator are prompted to change their passwords at their next login.

New passwords must meet the criteria dictated by the **local-user password** command options in the Global Configuration Mode.

Important The system does not allow the changing of passwords unless the time limit specified by the **local-user password min-change-interval** has been reached.

Example

The following command, executed by a security-administrator, resets the password for a local-user name *operator12*:

```
password change local-user operator12
```

patch plugin

Copies a patch intended for a specific plugin module onto the system. This function is associated with the patch process for accommodating dynamic software upgrades.

Product

ADC

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

patch plugin *plugin_name* binary_path **certificate** *certificate_path* **signature** *signature_path*

plugin_name

Specifies the name of an existing plugin that will be copied onto the system as an alphanumeric string of 1 through 16 characters.

certificate

Specifies the name of a certificate associated with the plugin that will be copied onto the system as an alphanumeric string of 1 through 16 characters.

filepath

Specifies the location of the file to copy. The path must be formatted as follows:

For the ASR 5000:

[file:]{ /flash | /pcmcia1 | /hd }[/*directory* **]/***file_name*

Important Use of the ASR 5000 SMC hard drive is not supported in this release.

For the ASR 5500:

[file:]{ /flash | /usb1 | /hd }[/*directory* **]/***file_name*

For VPC:

[file:]{ /flash | /hd-raid | /usb1 | usb2 | /cdrom1 }[/*directory* **]/***file_name*

Important The USB ports and CDROM must be configured via the hypervisor to be accessible.

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.

binary_path **certificate** ***certificate_path*** **signature** ***signature_path***

Validates signature along with P2P binary file for trusted builds. When P2P binary file (along with signature file) gets patched into the system, StarOS verifies the signature and accepts or rejects the P2P binary file. Verification is mandatory in trusted builds and is optional in normal builds.

Usage Guidelines

Use this command to verify and copy a patch onto the system. After the patch has been copied onto the system, you must run the **install plugin** command to unpack the kit and validate its contents.

Example

To copy the plugin module named *p2p* onto the system enter the following command:

```
patch plugin p2p http://192.168.1.2/tmp/libp2p-1.2.0.tgz certificate
http://192.168.1.2/tmp/1.2.0.cert
```

When the patch has been successfully copied the following message appears:

```
New patch for plugin p2p available for installation
```

ping

Verifies ability to communicate with a remote node in the network by passing data packets between and measuring the response. This is accomplished by sending IPv4 Internet Control Message Protocol (ICMP) echo request packets to the target node (pinging) and waiting for an ICMP response.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Important Inspector privileges are granted for all variables except **count**. To initiate a ping count, you must have a minimum privilege level of Operator.

Syntax Description

ping **(** *hostname* **|** *ip_address* **}** **[** **broadcast** **]** **[** **count** *num_packets* **]** **[** **df-bit** **{** **off** **|** **on** **}** **]** **[** **dscp** *dscp_value* **]** **[** **flood** **]** **[** **pattern** *packet_pattern* **]** **[** **size** *octet_count* **]** **[** **src** **{** *src_host_name* **|** *src_host_ip_address* **}** **]** **[** **vrf** *vrf_name*

hostname

Sends ICMP echo request packets to the remote node specified the node's name (up to 127 alphanumeric characters) or assigned IPv4 address in dotted-decimal notation.

ip_address

IPv4 address of host to be pinged in dotted-decimal notation.

broadcast

Sends ping packets to broadcast addresses.

count *num_packets*

Specifies the number of packets to send to the remote host for verification as an integer from 1 through 10000. Default: 5

df-bit { off | on }

Specifies whether or not the do-not-fragment bit will be included in the IP header.

dscp *dscp_value*

Specifies the 6-bit DSCP value as an integer from 0 through 63. Default: 0. The DSCP value must be previously mapped to an internal-class-of-service value using the Global Configuration mode **qos ip-dscp-iphb-mapping** command.

flood

Sends ping packets as rapidly as possible or 100 per second, whichever is faster.

Important Use with caution. Flood ping terminates after receiving (count) responses. If flood ping is used against an interface that is not responding, it will run indefinitely

pattern *packet_pattern*

Specifies a pattern to use to fill the internet control message protocol packets in hexadecimal format with a value in the range of 0x0000 through 0xFFFF. By default each octet of the packet is encoded with the octet number of the packet.

size *octet_count*

Specifies the number of bytes in each IP datagram as an integer from 40 through 18432. Default: 56

src *host_ip_address*

Specifies the source IP address in IPv4 dotted-decimal notation.Default: originating system's IP address

vrf *vrf_name*

Specifies the VRF name for which routing information will be displayed. *vrf_name* is an alphanumeric string of 1 through 63 characters.

Usage Guidelines

This command is useful in verifying network routing and if a remote node is able to respond at the IPv4 layer.

Example

The following command is the most basic and will report the results of trying to communication with remote node *remoteABC*.

```
ping remoteABC
```

The following command verifies communication with the remote node *209.165.200.229* using *1000* packets.

```
ping 209.165.200.229 count 1000
```

The following command verifies communication with remote node *remoteABC* while making it appears as though the source is remote node with IP address *209.165.200.229* .

```
ping remoteABC src 209.165.200.229
```

Important The responses from the remote host to the ping packets will be rerouted to the host specified as the source.

ping6

Verifies ability to communicate with a remote node in the network by passing data packets between and measuring the response. This is accomplished by sending IPv6 Internet Control Message Protocol (ICMP) echo request packets to the target node (pinging) and waiting for an ICMP response.

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

**ping6 { *hostname* | *ipv6_address* } [count *num*] [dscp *dscp_value*] [flood] [interface *interface_name*] [pattern *val*] [size *val*] [src *ip_address*] [vrf *vrf_name*

host_name

Name of the host to be pinged.

ipv6_address

IPv6 address of host to be pinged in colon-separated-hexadecimal notation.

count*num*

Sets the number of ping packets to be sent as an integer from 1 through 10000.

dscp *dscp_value*

Specifies the 6-bit DSCP value as an integer from 0 through 63. Default: 0. The DSCP value must be previously mapped to an internal-class-of-service value using the Global Configuration mode **qos ip-dscp-iphb-mapping** command.

flood

Configures ping6 to send packets as quickly as possible, or 100 per second, whichever is faster.

Important Use with caution. Flood ping terminates after receiving (count) responses. If flood ping is used against an interface that is not responding, it will run indefinitely

interface *interface_name*

Defines a named source interface from which ping packets will originate. *interface_name* is an alphanumeric string of 1 to 79 characters.

pattern *val*

Specifies the hexadecimal pattern to fill ICMP packets as a hexadecimal number from 0x0 through 0ffff

size *val*

Specifies the size of ICMP datagram (in bytes) as an integer from 40 through 18432. Default: 56.

src *ip_address*

Specifies the source IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. Default: originating system's IP address

vrf *name*

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

Usage Guidelines This command is useful in verifying network routing and if a remote node is able to respond at the IPv6 layer.

Example

Use this command to ping the IPv6 address *2001:0db8:85a3:0000:0000:8a2e:0370:7334*

```
ping6 2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

port disable, port enable

Disables or enables a port on a specified MIO/UMIO/MIO2 card without affecting the paired port on the other MIO/UMIO/MIO2 card. This capability is very useful in Active-Active LAG configurations on an ASR 5500.

Product All

Privilege Security Administrator, Administrator, Operator

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description **`port { disable | enable } ethernet`** *slot#*/*port#*

disable

Disables (shuts down) the specified MIO/UMIO/MIO2 port without disabling its paired port on the other MIO/UMIO/MIO2 card.

enable

Enables a previously disabled port on the specified MIO/UMIO/MIO2 port without affecting its paired port on the other MIO/UMIO/MIO2 card.

ethernet

Specifies the port type as Ethernet.

slot#

Identifies the physical chassis slot (5 or 6) where the MIO/UMIO/MIO2 card is installed.

port#

Identifies the physical port on the MIO/UMIO/MIO2 card to disable or enable.

Usage Guidelines

If you use the Ethernet Port Configuration mode **shutdown** command to shut down one of the ports on an MIO/UMIO/MIO2 card in an Active-Active LAG configuration, by default the paired port on the other MIO/UMIO/MIO2 card will also be shut down.

Use this command to disable (shut down) a port on an MIO/UMIO/MIO2 card without affecting the paired port on the other MIO/UMIO/MIO2 card in an Active-Active LAG configuration.

Example

The following command disables port 11 on the MIO card in slot 6.

```
port disable ethernet 6/11
```

port switch to

Performs a manual switchover to an available redundant/standby line card, SPIO port or MIO/MIO2 port.

Product

All

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

port switch to *slot#*/*port#*

slot#

Identifies the physical chassis slot where the line card, SPIO or MIO/MIO2 is installed.

port#

Identifies the physical port on the line card, SPIO or MIO/MIO2 to automatically switch to.

Usage Guidelines

This command is used to specify the redundant port on a Line Card (LC) or MIO/MIO2. When port redundancy is enabled, if an external network device or cable failure occurs that causes a link down failure on the port, then the redundant port is used.

Important This command is not supported on all platforms.

Example

On an ASR 5000 this command switched to port 17/1.

```
port switch to 17/1
```

On an ASR 5500 this command swithces to port 6/11.

```
port switch to 6/11
```

ppp echo-test

Sends link control protocol (LCP) keep-alive echo packet to the peer point-to-point protocol (PPP) connection to verify proper communication between PPP connections, and awaits a response.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
ppp echo-test { callid call_id | imsi imsi_id | ipaddr ip_address | msid ms_id
 | username user_name } [ num_packets ] [ | { grep grep_options | more } ]
```

callid *call_id*

Specifies the call instance ID for which the PPP link must be verified as a 4-byte hexadecimal number.

imsi *imsi_id*

Specifies the International Mobile Subscriber Identifier (IMSI) for which the PPP link must be verified.

ipaddr *ip_address*

Specifies the IP address for which the PPP link must be verified in IPv4 dotted-decimal notation.

msid *ms_id*

Specifies the mobile subscriber ID for which the PPP link must be verified as 7 to 16 digits of an MIN, or RMI.

username *user_name*

Specifies an existing user for which the PPP link must be verified as an alphanumeric string of 1 through 127 characters.

num_packets

Specifies the number of test packets to generate an integer from 1 through 1000000. Default: 1

grep *grep_options* | more

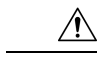
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

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

Usage Guidelines

Use this command to verify the point-to-point protocol communications. This command sends LCP keep-alive echo packet to the peer PPP connection to verify proper communication between PPP connections. **ppp echo-test** command waits for LCP echo response for configured numbers of tries, if response is not received it will retry configured no of times with an interval of 5 seconds. This command accepts the parameters call ID, IMSI, IP address, MSID, and user name to specify which active PPP session to consider.

ppp echo-test command makes the dormant session active.



Caution Issuing this command could negatively impact system performance depending on the number of subscribers using the same name and/or if the number of packets used in the test is large.

LCP includes Echo-Request and Echo-Reply codes in order to provide a Data Link Layer loopback mechanism for use in exercising both directions of the link. This is useful as an aid in debugging, link quality determination, performance testing, and for numerous other functions. Upon reception of an Echo-Request in the LCP Opened state, an Echo-Reply is transmitted.

Example

The following command tests the PPP link to user *user1*.

```
ppp echo-test username user1
```

The following command tests the PPP link to the user assigned IP address *209.165.200.229* .

```
ppp echo-test ipaddr 209.165.200.229
```

The following tests the PPP link associated with call ID *fe80AA12*.

```
ppp echo-test callid fe80aa12
```

push ssh-key

Pushes the secure shell (SSH) client public key to a remote server. The key must have been previously generated via the CLI commands in the SSH Client Configuration mode.

Product

All

Privilege

Security Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[context_name]host_name#`

Syntax Description

`push ssh-key { ` *`host_name`* **` | `** *`host_ip_address`* **` } user `** *`username`* **` [ context `** *`context_name`* **` ]`**

host_name

Specifies the remote server using its logical host name which must be resolved via DNS lookup. It is expressed as an alphanumeric string of 1 to 127 characters.

host_ip_address

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

user *username*

Specifies a valid username on the external server as an alphanumeric string of 1 to 79 characters.

context *context_name*

Specifies a valid StarOS context name. The context name is optional. If it is not provided the current context is used for processing.

Usage Guidelines

Use this command to push a public key to an external server. The SSH public key enables SSH access without a password between a StarOS gateway and the external server via the Exec mode **ssh** command. You must first create the SSH client key pair using CLI commands in the SSH Client Configuration mode.

Example

The following command pushes an SSH client public key to an external server named *remoteABC*.

```
push ssh-key remoteABC user admin012 context mme
```

radius interim accounting now

Check points current RADIUS Interim accounting messages immediately.

Product

PDSN

GGSN

ASN-GW

Privilege

Security Administrator, Administrator, Operator

Command Modes Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description **radius interim accounting now**

Usage Guidelines This command check points RADIUS Interim accounting as they are received. It is useful when preparing for system monitoring or troubleshooting.

Example

The following command initiates immediate checkpointing of RADIUS Interim accounting messages:

radius interim accounting now

radius test

Verifies the RADIUS servers functions for accounting and authentication.

Product PDSN

GGSN

ASN-GW

Privilege Security Administrator, Administrator, Operator

Command Modes Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description **radius test { accounting | admin authentication | authentication | probe authentication server** *ip_addr* **port** *port_no* **[username** *username* **password** *password* **] } { all | [on] | off] | radius group** *group_name user_name* **| server** *server_name* **port** *server_port* **}** *user_name password*

accounting

Tests accounting server functionality.

admin authentication *name_admin admin_password*

Tests the RADIUS admin authentication.

name_admin: Specifies he name of the administrator as an alphanumeric string of 1 through 127 characters.

admin_password: Specifies the password for the administrator as an alphanumeric string of 1 through 63 characters.

authentication

Tests authentication server functionality.

all | radius group *group_name user_name* | server *server_name* port *server_port*

all: Tests all configured servers.

server *server_name* **port** *server_port*: Tests only the server specified by *server_name* and *server_port*. The server must have been previously configured.

radius group *group_name user_name*: Tests all configured authentication servers in a specific RADIUS group for a specific user. Must be followed by the RADIUS group name and user name.

group_name is an alphanumeric string of 1 through 63 characters that specifies the name of server group configured in the specific context for authentication/accounting.

on/off

Allows the user to turn RADIUS test accounting on or off.

user_name

Specifies the RADIUS user who is to be verified. The user must have been previously configured.

password

Specifies the RADIUS user who is to have authentication verified. *password* is only applicable when the **authentication** keyword is specified.

Usage Guidelines

Test the RADIUS accounting for troubleshooting the system for specific users or to verify all the system RADIUS accounting functions.

Example

The following verifies all RADIUS servers.

```
radius test accounting all
```

```
radius test authentication all
```

The following verifies the RADIUS accounting and authentication for user **radius test authentication all***user1* for the *sampleServer*.

```
radius test accounting server sampleServer port 5000 user1
radius test authentication server sampleServer port 5000 user1 dumyPwd
```

The following commands will verify the RADIUS accounting and authentication for RADIUS server group *star1* for the current context:

```
radius test accounting server sampleServer port 5000 user1
```

```
radius test authentication server sampleServer port 5000 user1 dummyPwd
```

```
radius test authentication all
```

The following verifies the RADIUS authentication server group *star1* for user *user1*.

```
radius test authentication radius group star1 user1
```

reload

Invokes a full system reboot. All processes are terminated and the system initiates a hardware reset (reboot). This command is identical to the **shutdown** command.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
reload [ ignore-locks ] [ -noconfirm ]
```

ignore-locks

Reboots the system regardless of any save configuration operations that may be currently running. StarOS displays a warning message but does not wait for save configuration requests to complete before initiating the reboot.

```
Warning: One or more other administrators are saving configuration
```

Caution Use of the **ignore-locks** keyword may result in file corruption.

-noconfirm

Executes the command without any additional prompts or confirmation from the user.

Usage Guidelines

The system performs a hardware reset and reloads the highest priority boot image and configuration file specified in the boot.sys file. Refer to the **boot system priority** command in the Global Configuration Mode for additional information on configuring boot images, configuration files and priorities.

By default (without the **ignore-locks** option specified) **reload** waits for save configuration operations to complete before initiating the reboot.

Important To avoid the abrupt termination of subscriber sessions, it is recommended that a new call policy be configured and executed prior to invoking the **reload** command. This policy sets busy-out conditions for the system and allows active sessions to terminate gracefully. Refer to the **newcall** command in the Exec Mode for additional information.

Caution Issuing this command causes the system to become unavailable for session processing until the reboot process is complete.

Example

The following command performs a hardware reset on the system:

```
reload
```

rename

Changes the name of an existing local file.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

rename *from_filepath to_filepath* **[-noconfirm]**

from_filepath

Specifies the path to the file/directory to be renamed. The path must be formatted according to the following format:

For the ASR 5000:

[file:]{ /flash | /pcmcia1 | /hd-raid }[/*directory* **]/***file_name*

For the ASR 5500:

[file:]{ /flash | /usb1 | /hd-raid }[/*directory* **]/***file_name*

Important Use of the SMC hard drive is not supported in this release.

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

to_filepath

Specifies the path to the file/directory to be renamed. The path must be formatted according to the following format:

For the ASR 5000:

[file:]{ /flash | /pcmcia1 | /hd }[/*directory*]/*file_name*

Important Use of the SMC hard drive is not supported in this release.

For the ASR 5500:

[file:]{ /flash | /usb1 | /hd }[/*directory*]/*file_name*

directory is the directory name

filename is the actual file of interest

-noconfirm

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

Caution Extreme caution should be taken when using the **-noconfirm** option. The paths to the source and the destination should be verified prior to performing the command.

Usage Guidelines Rename files as part of regular system maintenance in conjunction with the delete command.

Example

The following renames the directory */pub* in the local PCMCIA1 device.

rename /pcmcia1/pub /pcmcia1/pub_old

The following renames the directory */pub* in the local USB device.

rename /usb1/pub /usb1/pub_old

reset active-charging

This command resets the active charging services.

Product All

Privilege Security Administrator, Administrator, Operator

Command Modes Exec

The following prompt is displayed in the Exec mode:

[local]*host_name*#

Syntax Description **reset active-charging credit-control misc-info max-backpressure { all | facility sessmgr instance** *instance_number* **}**

all

Displays the maximum backpressure information among all the active session manager instances.

facility sessmgr instance *instance_number*

Specifies the facility session manager instance as an integer ranging from 1 through 65535 characters.

Usage Guidelines

Use this CLI command to get or reset the maximum back-pressure hit and the timestamp it reached the maximum value. This helps to reset the gauge value for all/specific session manager instance to zero.

Example

The following command resets the maximum backpressure value for all active session manager instances:

```
reset active-charging credit-control misc-info max-backpressure all
```

reset alcap-service

Resets a named Access Link Control Application Part (ALCAP) protocol service. ALCAP is the protocol used for the control plane of the UMTS transport layer. It manges and multiplexes users into ATM AAL2 virtual connections.

Product

All (ASR 5000 only)

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

reset alcap-service *srvc_name* **aal2 node** *node_name* **aal2-path {** *path_name* **| all }**

srvc_name

Specifies the name of an existing ALCAP service as an alphanumeric string of 1 through 63 characters.

aal2 node *node_name*

Specifies the name of an existing ATM Adaptation Layer 2 (AAL2) node as an alphanumeric string of 1 through 64 characters.

Usage Guidelines

Reset a named ALCAP service for a specified AAL2 node.

Example

The following command resets the ALCAP service *alcap_01* for the AAL2 node *aal2_1001*, all paths:

```
reset alcap-service alcap_01 aal2-node aal2_1001 aal2-path all
```

reset diameter

This command clears the Diameter statistics.

Product

All

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`reset diameter aaa-statistics misc-data`

Usage Guidelines

Resets the Diameter statistics (highest backpressure statistics).

Example

The following command resets the Diameter related miscellaneous statistics:

`reset diameter aaa-statistics misc-data`

reset ims-authorization

Resets the maximum backpressure related information associated with the IMS authorization services.

Product

All

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`reset ims-authorization policy-control misc-info max-backpressure { all | facility sessmgr instance` *`instance_number`* **`}`**

all

Displays the maximum backpressure information among all the active session manager instances.

facility sessmgr instance *instance_number*

Specifies the facility session manager instance as a integer from 0 through 10000000 characters.

Usage Guidelines Use this command to reset the values of maximum backpressure related information.

Example

The following command resets all the backpressure related information:

```
reset ims-authorization policy-control misc-info max-backpressure all
```

reveal disabled commands

Enables or disables the input of commands for features that do not have license keys installed. The output of the command **show cli** indicates when this feature is enabled. This command effects the current CLI session only and is disabled by default.

Product All

Privilege Security Administrator, Administrator, Operator

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
[ no ] reveal disabled commands
```

no

Does not show disabled commands.

Important This command is not available in release 20.0 and higher Trusted builds.

Usage Guidelines When this command is enabled and a disabled command is entered, a message is displayed that informs you that the required feature is not enabled and also lists the name of the feature that you need to support the command.

When this command is disabled and a disabled command is entered, the CLI does not acknowledge the existence of the command and displays a message that the keyword is unrecognized.

Example

The following command sets the CLI to accept disabled commands and display the required feature for the current CLI session with the following command:

```
reveal disabled commands
```

The following command sets the CLI to reject disabled commands and return an error message for the current CLI session:

```
no reveal disabled commands
```

rlogin

Attempts to connect to a remote host.

Product

All

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

rlogin { *host_name* | *host_ip_address* } [user *user_name*]

host_name* | *host_ip_address

Identifies the remote node with which to attempt connection.

host_name: Specifies the remote node using the node's logical host name which must be resolved via DNS lookup.

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

user *user_name*

Specifies a user name attempting connection as an alphanumeric string of 1 through 1023 characters.

Usage Guidelines

Connect to remote network elements using rlogin.

Important **rlogin** is not a secure method of connecting to a remote host. **ssh** should be used whenever possible for security reasons.

Important The **rlogin** command is not available in Release 20.0 and higher Trusted builds.

Example

The following connects to remote host *remoteABC* as user *user1*.

```
rlogin remoteABC user user1
```

The following connects to remote host *10.2.3.4* without any default user.

```
rlogin 10.2.3.4
```

rmdir

Removes (deletes) a local directory.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`rmdir` *`path`* **`[ force ]`**

path

Specifies the directory path to remove. The must be formatted according as follows:

For the ASR 5000:

`[ file: ]{ /flash | /pcmcia1 | /hd-raid }[ /`*`directory`***` ]/`***`file_name`**

For the ASR 5500:

`[ file: ]{ /flash | /usb1 | /hd-raid }[ /`*`directory`***` ]/`***`file_name`**

For VPC:

`[ file: ]{ /flash | /hd-raid | /usb1 | /usb2 | /cdrom1 }[ /`*`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

force

Over-rides any warnings to force deletion of the directory and any files contained therein.

Important Use of the **force** keyword should be done with care to ensure the directory is specified accurately as there is no method to recover a directory which has been removed.

Usage Guidelines

Remove old directories as part of regular maintenance.

Example

The following removes the local directory */pcmcia1/pub*.

```
rmdir /pcmcia1/pub
```

rollback module

Loads a specified software plugin module from the Version Priority List (VPL) with the next higher priority number. This function is associated with the patch process for accommodating dynamic software upgrades.

Product

ADC

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

rollback module *plugin_name*

plugin_name

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

Usage Guidelines

Use this command to initiate a rollback of a previously loaded software plugin module. If it fails to load, the module with next highest priority will be loaded. If none of the modules are installed, the default patch which comes along with the ASR 5000 build is automatically loaded. The specified module must have been previously unpacked/verified and configured via the **install plugin** and **plugin** commands respectively.

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

Example

To load the next plugin module named *p2p* enter the following command:

```
rollback module p2p
```

rotate-hd-file

Rotates the Diameter files stored on the hard disk drive.

Product

HSGW

P-GW

SAEGW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`rotate-hd-file diameter [ name` *`policy_name`* **`]`**

name *policy_name*

Specifies the hd-storage policy name of an existing HD Storage Policy as an alphanumeric string of 0 through 63 characters.

Usage Guidelines

Use this command to manually rotate the Diameter HD stored files.

Example

The following command rotates Diameter files that were stored using the HD storage policy named CDR1:

`rotate-hd-file diameter name` *`CDR1`*

save configuration

Saves the configuration of current contexts to a local or remote location. The configuration contains the sequence of CLI commands that define system parameters and ends with the **.cfg** extension.

Important

In release 20.0 and higher Trusted StarOS builds, FTP is not supported. SFTP is the recommended file transfer protocol.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`save configuration` *`url`* **`[ confd | ignore-locks | obsolete-encryption | showsecrets | verbose ] [ -redundant ] [ -noconfirm ] [legacy-password-expiry]`**

url

Default: saves to the location of the active configuration currently loaded.

Specifies the location in which to store the configuration file. *url* may refer to a local or a remote file and must be entered in the following format:

For the ASR 5500:

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

For VPC:

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

Important Do not use the following characters when entering a string for the field names: "/" (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.

Important *host* can **only** be used if the **networkconfig** parameter is configured for DHCP and the DHCP server returns a valid nameserver.

The following file transfer protocols are supported on all platforms to save the configuration to a destination on the network (off box):

tftp – Trivial File Transfer Protocol [no username/password required]

ftp – File Transfer Protocol [username/password required]

sftp – SSH File Transfer Protocol [SSH username/password required]

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

[confd | ignore-locks | obsolete-encryption | showsecrets | verbose]

Specifies options when saving the configuration file.

confd: Saves only those configuration commands associated with the YANG model in support of Cisco NSO ConfD and the NETCONF protocol.

ignore-locks: Saves the configuration regardless of any configuration mode locks held by other administrative users or other external restrictions.

Important Use of the **ignore-locks** keyword may result in file corruption.

obsolete-encryption: Saves the configuration with encrypted values generated via an obsolete encryption method. This option may be required to preserve a configuration for a possible downgrade.

Important The **obsolete-encryption** keyword is only available in StarOS 19.1 and prior releases.

showsecrets: Saves the CLI configuration file with all passwords in plain text, rather than their default encrypted format.

Important The **showsecrets** keyword is only available in StarOS 19.1 and prior releases.

verbose: Saves as much information as possible, including default values. If this option is not specified, the configuration does not include default values.

legacy-password-expiry

Generates a backward compatible file by removing new Expiry Notification keywords, which were introduced as part of Password Expiry Notification Feature in StarOS 21.23 release. The new `save config` CLI option makes the configuration compatible with older StartOS versions in which the Password Expiry Notification Feature is not present.

-redundant

Saves the configuration file to the local device on the management card, defined by the *url* variable, and then automatically copies that same file to the like device on the standby management card, if available.

The management card can be any of the following:

- ASR 5500 – Management Input/Output (MIO/MIO2) card [/flash, usb1, usb2]
- VPC-DI – Control Function (CF) virtual machine

Use the **-redundant** keyword if you have only made changes to the configuration, but not to the boot order or after installing a new boot image. Changes to the boot order or installing a new image requires file synchronization via the **filesystem synchronize** command.

Important This keyword will only work for local devices on both the active and standby management cards. Otherwise, a failure message is displayed. When saving the file to an external network (non-local) device, the system disregards this keyword.

Important This keyword does not synchronize the local file system. If you have added, modified, or deleted other files or directories to or from a local device for the active management card, then synchronize the local file system on both cards.

-noconfirm

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

Caution Exercise caution when using the **-noconfirm** option as this overwritse data if the URL targets an existing file.

Usage Guidelines Backup the current configuration as part of periodic maintenance activities for emergency recovery.

Important Saving a configuration does not save the boot options as configured via the Global Configuration mode **boot** commands.

Example

The following command saves the configuration data to the local file */flash/pub/juneconfig.cfg* with no confirmation from the user:

```
save configuration /flash/pub/juneconfig.cfg -noconfirm
```

The following command saves the configuration data to remote host *remoteABC* at */pub/juneconfig.cfg*:

```
save configuration tftp://remoteABC/pub/juneconfig.cfg
```

The following command saves only those configuration commands associated with the YANG model in support of Cisco NSO ConfD and the NETCONF protocol:

```
save configuration confd /flash/netconf/confd.cfg
```

The following command generates a backward compatible file by removing new Expiry Notification keywords:

```
save config /flash/start-downgrade-20211012-c-op.cfg legacy-password-expiry
```

save logs

Saves the current log file to a local or remote location.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

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

url

Specifies the location to store the log file(s). *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-raid } [/*directory* **] /***file_name*
tftp:// { ***host* **[: ***port#* **] } [/*directory* **] /***file_name*
[ftp: | sftp:] // [***username*[:***password* **] @] { ***host* **} [: ***port#* **] [/***directory* **] / ***file_name*

Important Use of the SMC hard drive is not supported in this release.

For the ASR 5500:

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

For VPC:

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

Important The USB ports and CDROM must be configured via the hypervisor to be accessible.

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.

Important *hostname* can only be used if the **networkconfig** parameter is configured for DHCP and the DHCP server returns a valid nameserver.

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

active

Saves data from active logs.

inactive

Saves data from inactive logs.

callid *call_id*

Specifies a call ID for which log information is to be saved as a 4-byte hexadecimal number.

event-verbosity *evt_verboseness*

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

- *min*: Logs minimal information about the event. Information includes event name, facility, event ID, severity level, date, and time.
- *concise*: Logs detailed information about the event, but does not provide the event source within the system.
- *full*: Logs 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. Valid facilities for this command are:

- **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)
- **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]
- **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
- **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
- **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*

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

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

pdu-data *pdu_format*

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

- *none* - raw format (unformatted).
- *hex* - hexadecimal format.
- *hex-ascii* - 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 a value from 1 to 5, where 5 is the most detailed.

since *from_date_time* [until *to_date_time*]

Default: no limit.

since *from_date_time*: Saves only the log information which has been collected more recently than *from_date_time*.

until *to_date_time*: Saves no log information more recent than *to_date_time*. 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*.

Using the **until** keyword allows for a time range of log information; using only 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 in *Command Line Interface Reference*.

Usage Guidelines

Backup the current log file as part of periodic maintenance activities.

Example

The following saves the log to the local file */flash/pub/junelogs.logs* with no confirmation from the user:

```
save logs /flash/pub/junelogs.logs -noconfirm
```

The following saves the configuration data to remote host *remoteABC* as */pub/junelogs.logs*:

```
save logs tftp://remoteABC/pub/junelogs.logs
```

session trace

Enable or disables the subscriber session trace functionality based on a specified subscriber device or ID on one or all instance of session on a specified UMTS/EPS network element. It also clears/resets the statistics collected for subscriber session trace on a system.

Product

GGSN

MME

P-GW

SAEGW

S-GW

Privilege

Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

session trace { reset statistics | subscriber network-element { mme | pgw | sgw | ggsn saegw [func-pgw | func-sgw } { imei *id* **| imsi** *id* **| interface { all |** *interface* **} | target-all-ne | target-ne { enb [target-interface { all |** *interface* **}] | pgw [target-interface { all |** *interface* **}] | sgw [target-interface { all |** *interface* **] } } trace-ref** *id* **collection-entity** *ip_address*

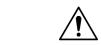
no session trace subscriber network-element [mme | pgw | sgw | ggsn] [trace-ref *id* **]**

no

Disables the entire session trace or for a specific network element and/or trace reference.

reset statistics

Clears/resets the entire session trace statistical data collected on a system.



Caution This is a system wide command that affects all statistical data.

session trace subscriber network-element { mme | pgw | sgw | ggsn }

Identifies the network element that, in turn, identifies the interfaces where the session trace is to occur. Specific interfaces can be specified using the interface keyword described below.

ggsn: Specifies that the session trace is to occur on one or all interfaces on the GGSN.

mme: Specifies that the session trace is to occur on one or all interfaces on the MME.

pgw: Specifies that the session trace is to occur on one or all interfaces on the P-GW.

sgw: Specifies that the session trace is to occur on one or all interfaces on the S-GW.

imei *id*

Specifies the International Mobile Equipment Identification number of the subscriber UE. *id* must be the 8-digit TAC (Type Allocation Code) and 6-digit serial number. Only the first 14 digits of the IMEI/IMEISV are used to find the equipment ID.

imsi *id*

Specifies the International Mobile Subscriber Identification (IMSI). *id* must be the 3-digit MCC (Mobile Country Code), 2- or 3- digit MNC (Mobile Network Code), and the MSIN (Mobile Subscriber Identification Number). The total should not exceed 15 digits.

interface { all | *interface* }

Specifies the interfaces where the session trace application will collect data.

all: Specifies all interfaces associated with the selected network element

interface: Specifies the interface type where the session trace application will collect trace data. The following interfaces are applicable for each network element type:

GGSN:

- **gi**: Specifies that the interface where the trace will be performed is the Gi interface between the GGSN and RADIUS server.
- **gmb**: Specifies that the interface where the trace will be performed is the Gmb interface between the GGSN and BM-SC.
- **gn**: Specifies that the interface where the trace will be performed is the Gn interface between the GGSN and the SGSN.
- **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the GGSN and PCRF.
- **gy**: Specifies that the interface where the trace will be performed is the Gy interface between the GGSN and OCS.

MME:

- **s1mme**: Specifies that the interface where the trace will be performed is the S1-MME interface between the MME and the eNodeB.
- **s3**: Specifies that the interface where the trace will be performed is the S3 interface between the MME and an SGSN.
- **s6a**: Specifies that the interface where the trace will be performed is the S6a interface between the MME and the HSS.
- **s10**: Specifies that the interface where the trace will be performed is the S10 interface between the MME and another MME.
- **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the MME and the S-GW.
- **s13**: Specifies that the interface where the trace will be performed is the S13 interface between the MME and the EIR.

P-GW:

- **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
- **gy**: Specifies that the interface where the trace will be performed is the Gy interface between the P-GW and OCS.

- **s2a**: Specifies that the interface where the trace will be performed is the S2a interface between the P-GW and the HSGW.
- **s2b**: Specifies that the interface where the trace will be performed is the S2b interface between the P-GW and an ePDG.
- **s2c**: Specifies that the interface where the trace will be performed is the S2c interface between the P-GW and a trusted, non-3GPP access device.
- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the P-GW and the S-GW.
- **s6b**: Specifies that the interface where the trace will be performed is the S6b interface between the P-GW and the 3GPP AAA server.
- **s8b**: Specifies that the interface where the trace will be performed is the S8b interface between the P-GW and the S-GW.
- **sgi**: Specifies that the interface where the trace will be performed is the SGi interface between the P-GW and the PDN.

S-GW:

- **gxc**: Specifies that the interface where the trace will be performed is the Gxc interface between the S-GW and the PCRF.
- **gy**: Specifies that the interface where the trace will be performed is the Gy interface between the S-GW and OCS.
- **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the S-GW and the MME.
- **s4**: Specifies that the interface where the trace will be performed is the S4 interface between the S-GW and an SGSN.
- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the S-GW and the P-GW.
- **s8b**: Specifies that the interface where the trace will be performed is the S8b interface between the S-GW and the P-GW.

target-all-ne

This option is applicable for MME only. Specifies that the trace be propogated to neighboring Network Elements (NEs) including the eNodeB, P-GW and S-GW. With this option, tracing will occur on all applicable interfaces on the respective NEs.

target-ne { enb [target-interface { all | *interface* }] | pgw [target-interface { all | *interface* }] | sgw [target-interface { all | *interface*] }

This option is applicable for MME only.

The **target-ne { enb | pgw | sgw }** keyword specifies that the trace be propogated to the specified neighboring Network Elements (NE). More than one **target-ne** can be configured in the same command.

target-interface { all | *interface* **}**: This optional keyword specifies the interface on the target NE where the trace will be performed. Multiple target-interfaces can be defined within the same command.

trace-ref *id*

Specifies the trace reference for the trace being initiated. *id* must be the MCC (3 digits), followed by the MNC (3 digits), then the trace ID number (3-byte octet string).

collection-entity *ip_address*

Specifies the IP address of the collection entity where session trace data is pushed in IPv4 dotted-decimal notation.

Usage Guidelines

Use this command to initiate a session trace for a specified subscriber device or ID on one or all interfaces on a specified network element.

Important Session trace configuration is performed in the *Global Configuration Mode* using the **session trace** command. Refer to the *Global Configuration Mode Commands* chapter for more information.

Example

The following command initiates a session trace on a P-GW S5 interface for a subscriber with an IMSI of *322233123456789* and sets the trace reference as *322233987654* and the collection entity IP address as *209.165.200.229* :

```
session trace subscriber network-element pgw imsi 322233123456789 interface
 s5 trace-ref 322233987654 collection-entity 209.165.200.229
```

The following command initiates a session trace on an MME S6a interface for a subscriber with an IMSI of *322233123456789* and sets the trace reference as *322233987654* and the collection entity IP address as *209.165.200.229* :

```
session trace subscriber network-element mme imsi 322233123456789 interface
 s6a trace-ref 322233987654 collection-entity 209.165.200.229
```

The following command initiates a session trace on a Gn interface on GGSN between GGSN and SGSN for a subscriber with an IMSI of *322233123456789* and sets the trace reference as *322233987654* and the collection entity IP address as *209.165.200.229* :

```
session trace subscriber network-element ggsn imsi 322233123456789
interface gn trace-ref 322233987654 collection-entity 209.165.200.229
```

MME Only: The following command activates a session trace on S-GW for S5 interface from the MME:

```
session trace subscriber network-element mme imsi 0000012345 target-ne
sgw target-interface s5
```

session trace random

Enable or disables the subscriber session trace functionality based on a the random trace on the network element. If enabled, the subscriber selection will be based on random logic all instance of session on a specified UMTS/EPS network element. It also clears/resets the statistics collected for subscriber session trace on a system.

Product

GGSN

P-GW

Privilege

Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`[no] session trace random` *`random_num`* **`network-element {ggsn | pgw} [interface {all |`** *`interface`***`]`**

no

Disables the entire random subscriber session trace or for a specific network element and/or interface.

session trace random *random_num*}

Configures the number of random subscriber sessions where the session trace is to occur.

random_num is an integer between 1 to 1000 identified the number of subscribers to be selected by random logic.

network-element {ggsn | pgw}

Identifies the network element that, in turn, identifies the interfaces where the random session trace is to occur. Specific interfaces can be specified using the interface keyword described below.

ggsn: Specifies that the random session trace is to occur on one or all interfaces on the GGSN.

pgw: Specifies that the random session trace is to occur on one or all interfaces on the P-GW.

interface { all | *interface* }

Specifies the interfaces where the random session trace application will collect data.

all: Specifies all interfaces associated with the selected network element

interface: Specifies the interface type where the random session trace application will collect trace data. The following interfaces are applicable for the network element type:

- GGSN:
  - **gi**: Specifies that the interface where the trace will be performed is the Gi interface between the GGSN and RADIUS server.
  - **gmb**: Specifies that the interface where the trace will be performed is the Gmb interface between the GGSN and BM-SC.
  - **gn**: Specifies that the interface where the trace will be performed is the Gn interface between the GGSN and the SGSN.
  - **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the GGSN and PCRF.

- **gy**: Specifies that the interface where the trace will be performed is the Gy interface between the GGSN and Diameter.

- P-GW:
  - **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
  - **gy**: Specifies that the interface where the trace will be performed is the Gy interface between the GGSN and Diameter.
  - **s2a**: Specifies that the interface where the trace will be performed is the S2a interface between the P-GW and the HSGW.
  - **s2b**: Specifies that the interface where the trace will be performed is the S2b interface between the P-GW and an ePDG.
  - **s2c**: Specifies that the interface where the trace will be performed is the S2c interface between the P-GW and a trusted, non-3GPP access device.
  - **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the P-GW and the S-GW.
  - **s6b**: Specifies that the interface where the trace will be performed is the S6b interface between the P-GW and the 3GPP AAA server.
  - **s8b**: Specifies that the interface where the trace will be performed is the S8b interface between the P-GW and the S-GW.
  - **sgi**: Specifies that the interface where the trace will be performed is the SGi interface between the P-GW and the PDN.

Usage Guidelines Use this command to initiate the session trace for a specified subscriber sessions selected on random logic on one or all interfaces on a specified network element.

Important Session trace configuration is performed in the *Global Configuration Mode* using the **session trace** command. Refer to the *Global Configuration Mode Commands* chapter for more information.

Example

The following command initiates a session trace on a GGSN Gx interface for *1000* subscriber session selected on random logic:

```
session trace random 1000 network-element ggsn interface gx
```

session trace signaling

Enable or disables the subscriber session trace functionality based on signaling information on one or all instance of session on a specified UMTS/EPS network element. It also clears/resets the statistics collected for subscriber session trace on a system.

Product

GGSN

P-GW

Privilege

Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`[no] session trace signaling network-element {ggsn | pgw}`

no

Disables the entire session trace based on signaling information for a specific network element and/or trace reference.

session trace signaling network-element {pgw | ggsn}

Identifies the network element that where the session trace based on signaling information for a subscriber session is to occur. Specific network element GPRS/EPS can be specified for this session trace.

ggsn: Specifies that the session trace based on signaling is to occur on one or all interfaces on the GGSN.

pgw: Specifies that the session trace based on signaling is to occur on one or all interfaces on the P-GW.

Usage Guidelines

Use this command to initiate a session trace for a specified subscriber based on signaling information on a specified network element.

Important Session trace configuration is performed in the *Global Configuration Mode* using the **session trace** command. Refer to the *Global Configuration Mode Commands* chapter for more information.

Example

The following command initiates a session trace on a GGSN for a subscriber based on signaling information.

`session trace signaling network-element ggsn`

setup

Enters the system setup wizard which guides the user through a series of questions regarding the system basic configuration options, such as initial context-level administrative users, host name, etc.

Product

All

Privilege

Security Administrator, Administrator

Command Modes Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description **`setup`**

Usage Guidelines The setup wizard provides a user friendly interface for initial system configuration.

Important If the configuration script generated by the setup wizard is applied when an existing configuration is in use, the options which are common to both are updated and all remaining options are left unchanged.

Example

The following command starts the setup wizard:

`setup`

sgs offload

Enables or disables offloading of UEs associated with a VLR which has become unavailable. This enables the MME to preemptively move subscribers away from a VLR which is scheduled to be put in maintenance mode.

Product MME

Privilege Security Administrator, Administrator

Command Modes Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description **`sgs offload sgs-service`** *`sgs_svc_name`* **`vlr`** *`vlr_name`* **`{ start time-duration`** *`minutes`* **`| stop } [ -noconfirm ]`**

sgs-service *sgs_svc_name*

Specifies the SGs service to which the VLR belongs.

sgs_svc_name specifies the name of a pre-configured SGs service. For more information on the SGs service, refer to the **sgs-service** command in the *Context Configuration Mode Commands* chapter and refer to the *MME SGs Service Configuration Mode Commands* chapter.

vlr *vlr_name*

Specifies the VLR service which must have its UEs offloaded.

vlr_name specifies the name for a pre-configured VLR and must be an alphanumeric string of 1 through 63 characters. For more information, refer to the **vlr** command in the *MME SGs Service Configuration Mode Commands* chapter.

start time-duration *minutes*

Specifies that the UE offloading should be started for the specified the VLR.

time-duration defines the period in *minutes* over which all qualifying subscribers will be offloaded.

minutes must be an integer from 0 to 3000.

A value of 0 enables only Passive VLR Offloading, where the MME marks all affected session manager with the "VLR Offload" flag. During the next UE activity, the MME requires each UE to perform a combined TAU/LAU. This flag is not affected by the removal of the "offload" state by the operator. Even though the VLR state may later change from "offloaded' to "not-offloaded", the subscriber's state will not change to "not-offloaded".

A value of 1-3000 enables Active VLR Offloading and Passive VLR Offloading. The MME splits this time-duration into *n* intervals, 5 seconds apart. A maximum of 50 subscribers will be actively detached per interval. For example, a setting of 5 minutes with 600 subscribers in a sessmgr (from the given VLR) would detach 10 subscribers per 5-second interval. Node level detach rate should be estimated by taking into account the number of sessmgr tasks. Any subscribers remaining at the expiry of the time-duration will not be detached.

Note: For Release 12.2, only Passive VLR Offloading is supported. While the **time-duration** value is not used in Release 12.2 or earlier, it is required for completion of the **start** command.

stop

Specifies that the offload state should no longer be set for the specified the VLR.

-noconfirm

Indicates that the command is to execute without additional prompt and confirmation from the user.

Usage Guidelines

This command enables the MME to preemptively move subscribers away from a VLR which is scheduled to be put in maintenance mode. When this offload command is set on the MME, all session manager matching this VLR are marked with an "offload" flag. If the time-duration keyword is set to 1-3000, session manager are also detached and required to reattach.

The configured time-duration is used to explicitly detach the subscriber in a specified rate. Upon expiry of the timer, the offload state of the VLR will not be changed and the offloading must be stopped by explicitly triggering the "stop" option.

The behavior of SGs with respect to "Location Updates" towards the MSC is similar to the behavior when the "VLR Reliable" flag is set to "false". In other words, for offloaded subscribers, normal Combined TAUs (without IMSI Attach) and periodic TAUs will trigger a LU towards the MSC.

When issuing the command, the MME notifies the operator if this is the last available VLR in a pool.

More than one VLR may be offloaded at the same time.

VLR Offloading and MME offloading cannot be performed at the same time.

Important This is a licensed feature and is unavailable unless the proper licensed is installed.

Related Commands:

- To display VLR offload information and statistics for a specified SGs service name, refer to the **show sgs-service offload-status service-name** *sgs_svc_name* command.
- To clear the counters displayed by the previous command, issue the **clear sgs-service statistics service-name** *sgs_svc_name* command.

Example

The following command starts offloading the subscribers associated with *vlr1* over the next 60 minutes.

```
sgs offload sgs-service sgs1 vlr vlr1 start time-duration 60 -noconfirm
```

sgs vlr-failure

This command configures the MME to monitor all VLRs and perform a controlled release (detach) of affected UEs when any VLR becomes unavailable.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

sgs vlr-failure sgs-service *sgs_svc_name* **duration** *minutes* **backoff-timer** *seconds* **[-noconfirm]**

no sgs vlr-failure sgs-service *sgs_svc_name*

no

Resets the command to its default setting of disabled.

sgs

Specifies SGS exec commands.

vlr-failure

Specifies VLR failure configuration.

sgs-service *sgs_svc_name*

Specifies the name of a pre-configured SGs Service to which the VLR belongs.

sgs_svc_name must be a string of size 1 to 63.

duration *minutes*

Specifies the amount of time in minutes during which all qualifying UEs will be detached.

The MME splits this duration into *n* intervals, 5 seconds apart. A maximum of 50 subscribers are processed per interval per session manager. For example, a setting of 5 minutes with 600 subscribers in a session manager (from a given VLR) would result in the session manager processing 10 subscribers per 5-second interval. Node level detach rate should be estimated by taking into account the number of sessmgr tasks. Any subscribers remaining at the expiry of the duration will not be processed.

minutes must be an integer from 1 through 3000.

backoff-timer *seconds*

Specifies the period of time the MME will wait following the detection of a VLR condition before starting the controlled release of affected UEs.

Specifies the backoff timer in seconds.

seconds must be an integer from 1 to 3000.

-noconfirm

Indicates that the command is to execute without additional prompt and confirmation from the user.

Usage Guidelines

When this command is issued, the MME monitors the availability of all VLRs. If one or more VLRs become unavailable, the MME performs a controlled release (EPS IMSI detach) for all UEs associated with that VLR. If another VLR is available, the MME sends a combined TA/LA Update with IMSI attach.

This command remains active until it is disabled with the **no sgs vlr-failure** command.

Important This is a licensed feature and is unavailable unless the proper licensed is installed.

Related Commands:

- To display VLR failure information and statistics, refer to the **show sgs-service vlr-status full** command.

Example

The following enables the monitoring and automatic detach of UEs when any VLR becomes unavailable. The MME will wait 2 minutes (120 seconds) after detecting a VLR condition before starting the controlled release of the affected UEs. The MME will process the UEs over a span of 60 minutes.

```
sgs vlr-failure sgs-service sgs1 duration 60 backoff-timer 120 -noconfirm
```

sgs vlr-recover

This command enables active recovery of Circuit Switched Fall Back (SMS-only) UEs when a failed VLR becomes responsive again.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`[no] sgs vlr-recover sgs-service` *`sgs_svc_name`* **`duration`** *`minutes`* **`backoff-timer`** *`seconds`***`[ -noconfirm ]`**

no

Resets the command to its default setting of disabled.

sgs-service *sgs_svc_name*

Specifies the SGs service to which the VLR belongs.

sgs_svc_name specifies the name for a pre-configured SGs service.

duration *minutes*

Specifies the amount of time in minutes over which all qualifying UEs will be recovered.

The MME splits this duration into *n* intervals, 5 seconds apart. A maximum of 50 subscribers will be processed per interval per session manager. For example, a setting of 5 minutes with 600 subscribers in a session manager (from a given VLR) would result in the session manager processing 10 subscribers per 5-second interval. Node level detach rate should be estimated by taking into account the number of session manager tasks. Any subscribers remaining at the expiry of the duration will not be processed.

minutes must be an integer from 1 through 3000.

backoff-timer *seconds*

Specifies the period of time the MME will wait following the detection of a recovered VLR before starting the VLR recovery actions.

seconds must be an integer from 1 to 3000.

-noconfirm

Indicates that the command is to execute without additional prompt and confirmation from the user.

Usage Guidelines

When this command is issued, the MME monitors the availability of all VLRs. If a failed VLRs become available again, the MME attempts to recover CSFB (SMS-only) UEs that failed while the VLR was unavailable with an EPS Detach.

Important This is a licensed feature and is unavailable unless the proper licensed is installed.

Related Commands:

- To display VLR recovery information and statistics, refer to the **show sgs-service vlr-status full** command.

Example

The following enables the active recovery of Circuit Switched Fall Back (SMS-only) UEs when a failed VLR becomes responsive again. The MME will wait 2 minutes (120 seconds) after detecting a recovered VLR before starting the recovery of the affected UEs. The MME will process the UEs over a span of 60 minutes.

```
sgs vlr-recover sgs-service sgs1 duration 60 backoff-timer 120 -noconfirm
```

sgsn clear-congestion

This command clears (terminates) congestion triggered using the **sgsn trigger-congestion** command.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
sgsn clear-congestion
```

Usage Guidelines

This command is only used if the **sgsn trigger-congestion** command has been issued in an OAM scenario. This **sgsn clear-congestion** command causes the SGSN to resume normal operations and does not apply any congestion control policy.

Example

Clear the triggered congestion on the SGSN.

```
sgsn clear-congestion
```

sgsn clear-detached-subscriptions

Clears subscription data belonging to a subscriber who has already detached.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

sgsn clear-detached-subscriptions imsi *imsi*

imsi *imsi*

Specifies the international mobile subscriber identity (IMSI) of the subscriber session identifying the subscription data to be cleared.

Usage Guidelines

This command can be issued on either a 2G or 3G SGSN to clear subscription data (including subscription information, and information for P-TMSI allocated, received authorization vectors, and NGAF flag values). This command is only effective if the subscriber has already detached.

After the data is purged, the SGSN sends an appropriate message to the HLR.

Related Commands:

- To clear subscription data for subscribers that are currently attached, refer to the **admin-disconnect-behavior clear-subscription** commands described in the chapters for *GPRS Service Configuration Mode* or the *SGSN Service Configuration Mode*.

Example

sgsn clear-detached-subscriptions imsi 040501414199978

sgsn imsimgr

Initiates an audit for managing the SGSN's IMSI manager's (IMSIMgr) IMSI table.

Important These commands are used primarily for troubleshooting purposes and are intended for the use of specially trained service representatives.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

sgsn imsimgr { instance *instance_id* **}{ add-record***imsi* **sessmgr instance** *sessmgr#* **| audit-with sessmgr { all | instance** *sessmgr#* **} | remove-record** *imsi* **}**

instance *instance_id*

The number of IMSI Managers supported is scaled up to "4" on ASR 5500 and a VPC-DI platforms. This keyword is used to specify the IMSI manager instance for which the audit is initiated. The audit is initiated

from only one specified instance of IMSI Manager at a time. This feature is only supported on ASR5500 and VPC-DI platforms.

instance_id: The *instance_id* is an integer from 1 through 4, it identifies the IMSI Manager instance for which the audit is initiated.

add-record *imsi*

Adds a record for an IMSI to the IMSI manager's table and associates a specific session manager (SessMgr) with the IMSI.

imsi: Enter up to 15 digits. An IMSI consists of the 3-digit MCC (mobile country code) + the 2- or 3-digit MNC (mobile network code) + the MSIN (mobile station identification number) for the remaining 10 or 9 digits (depending on the length of the MNC).

audit-with

Initiates an IMSI audit with all SessMgrs or a Session Manager (SessMgr) instance specified.

remove-record *imsi*

Deletes a specific IMSI from the IMSI table.

imsi: Enter up to 15 digits. An IMSI consists of the 3-digit MCC (mobile country code) + the 2- or 3-digit MNC (mobile network code) + the MSIN (mobile station identification number) for the remaining 10 or 9 digits (depending on the length of the MNC).

sessmgr instance *sessmgr#*

For releases prior to 14.0, this keyword specifies a Session Manager (SessMgr) instance associated with the IMSI as an integer from 0 through 4095.

For releases 14.0 and later, this keyword specifies a Session Manager (SessMgr) instance associated with the IMSI as an integer from 0 through 384.

Usage Guidelines

Use this command to manage the IMSIMgr's IMSI table, and to initiate an audit of one or more SessMgrs with the IMSIMgr so that the IMSI table has the correct IMSI-SessMgr association. After this audit, any IMSI in the IMSIMGR which is not found in any Sessmgr is deleted and similarly any missing entries at the IMSIMgr are created.

Example

Delete IMSI *044133255524211* from the audit table:

```
sgsn imsimgr remove-record 044133255524211
```

sgsn offload

Instructs the SGSN to begin the offloading procedure and actually starts and stops the offloading of subscribers which is part of the SGSN Gb (2G) or Iu (3G) Flex load redistribution functionality.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

sgsn offload { gprs-service *service_name* **| sgsn-service** *service_name* **} { activating [imsi** *imsi* **| nri-value** *nri_value* **| stop [imsi** *imsi* **| nri-value** *nri_value* **]] | connecting [nri-value** *nri_value* **| stop [imsi** *imsi* **| nri-value** *nri_value* **| target-nri** *target_nri* **] | t3312-timeout** *seconds* **[nri-value** *nri_value* **| target-nri** *target_nri* **] | target-nri** *target_nri* **[imsi** *imsi* **| target-count** *num_to_offload* **] }**

gprs-service *srvc_name*

Specifies a unique alphanumeric string of 1 through 63 characters that identifies a GPRS service that has already been defined for the 2G SGSN configuration.

sgsn-service *srvc_name*

Specifies a unique alphanumeric string of 1 through 63 characters that identifies an SGSN service that has already been defined for the 3G SGSN configuration.

activating

Instructs the SGSN to off load any subscribers sending an "activate request" message.

connecting

Instructs the SGSN to off load any subscribers sending either an Attach Request or a RAU Request message. Including this keyword without adding the **target-nri** and **target-count** keywords activates local offloading.

imsi *imsi*

Identifies a subscriber by the international mobile subscriber ID (IMSI) which consists of the 3-digit MCC (mobile country code) + the 2- or 3-digit MNC (mobile network code) + the MSIN (mobile station identification number) for the remaining 10 or 9 digits (depending on the length of the MNC).

imsi- enter an integer comprising up to 15 digits.

nri-value *nri-value*

Sets the local NRI. Including this keyword in the configuration instructs the SGSN to check the P-TMSI and use the SGSN matching the configured NRI value to off load subscribers.

Important **nri-value** and **target-nri** are mutually exclusive.

nri-value is an integer from 1 through 63 that identifies a specific, already defined, SGSN in a pool. (NRI defined in the service configuration.)

Use of 0 (zero) value is not recommended.

stop

Instructs the SGSN to stop offloading subscribers from the pool area.

target-nri *target_nri*

Instructs the SGSN to begin dynamically load balancing across a network of pooled SGSNs.

target_nri is an integer from 0 through 63 that identifies an already defined target NRI (SGSN) to which the subscribers are to be offloaded. (NRI previously defined in the service configuration.)

Use of 0 (zero) value is not recommended.

target-count *target_count*

Identifies the number of subscribers to be offloaded as an integer from 0 through 4000000. Instructs the SGSN to begin target count-based offloading.

t3312-timeout *seconds*

Sets the timer (in seconds) for sending period RAUs to the MS as an integer from 2 through 60. Default: 4

Usage Guidelines

Use this command to configure the offloading of subscribers which is a part of the SGSN's load redistribution operation. This command can be used anytime an SGSN is to be taken out of service.

Commands, with different NRI values, are repeated to expand/contract the radius of the offloading.

Target count-based offloading and local offloading can not run simultaneously. When target count offloading is to be used, you should choose an algorithm to control offloading from the perspective of the IMSIMGR and SESSMGR. This is done with the **target-offloading** command in the SGSN-Global configuration mode.

Example

The following two commands initiate **local offloading**.

Command 1: The following command instructs the SGSN to begin local offloading for the local NRI id *1* included in the *gprs1* GPRS service configuration:

```
sgsn offload gprs-service gprs1 connecting nri-value 1
```

Command 2: Enter this second command to add offloading for NRI *2* to the offloading already occurring for NRI *1*:

```
sgsn offload gprs-service gprs1 connecting nri-value 2
```

The following two commands discontinue local offloading and initiate **target count-based offloading.**

Command 1: The following command instructs the SGSN to discontinue local offloading for NRIs *5* included in the *sgsnserv4* SGSN service configuration :

```
sgsn offload sgsn-service sgsnserv4 connecting stop nri 5
```

Important The next command is an example of provision configuration for multiple NRI with a single command.

Command 2: The following command instructs the SGSN to initiate target count-based offloading for target NRI *5* to a target count of *10000* and target NRI *6* to count of *300000*:

```
sgsn offload sgsn-service sgsnserv4 connecting target-nri 5 target-count
 100000 target-nri 6 target-count 300000
```

sgsn op

Instructs the SGSN to begin specific operations or functions.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`sgsn op { auth-ptmsi-counters imsi` *`imsi`* **`| convert | nse { fr | ip | sgsn-invoke-trace } | show | ss7-rd`** *`ss7-rd_id`* **`{ destination | link | linkset | peer } }`**

auth-ptmsi-counters imsi *imsi*

Displays the authentication, P-TMSI reallocation, and P-TMSI signature reallocation counters for the specified IMSI.

imsi: Enter a unique 15-digit number associated with a mobile phone.

convert point-code *pt_code* variant *variant*

Converts SS7 point codes, according to identified variants, from dotted-decimal format to decimal format and vice versa.

point-code *pt_code*: Enters an SS7 point code in either dotted-decimal format or decimal format.

variant *variant*: Identifies the appropriate variant for the point code:

- **ansi**
- **itu**
- **ttc**

nse { fr *operation* | ip *operation* | sgsn-invoke-trace nse-id *nse_id* }

Enables the operator to perform a range of live control functions (for example, reset, block, unblock) for various types of virtual connections based on the signalling type of the NSE:

fr: Identifies a Frame Relay NSE.

ip: Identifies an IP NSE.

operation: Identifies the operation to be performed for the NSE connection (if available for the selected signalling type):

- **block nse-id** *nse_id*: Blocks signal flow through all network service virtual connections (NSVC) for the specified NSE:
  - *nse_id*: an integer from 0 to 65535.
- **bvc-flc-limit rate** *rate* **bvc-id** *bvc_id* **nse-id** *nse_id* - SGSN initiates flow control at the defined percentage rate to limit the flow through the BSSGP virtual connection (BVC) for the specified NSE and optionally for a specified BVC.
  - *rate*: an integer from 0 to 100.
  - *bvc_id*: an integer from 0 to 65000.
  - *nse_id*: an integer from 0 to 65535.
- **bvc-reset bvc-id** *bvc_id* **nse-id** *nse_id*: SGSN initiates a BVC-Reset on the specified BVC and NSE:
  - *bvc_id*: an integer from 0 through 65000.
  - *nse_id*: an integer from 0 through 65535.
- **nsvc** *nsvc_id* **{ block | enable | disable | unblock }***nse_id* - SGSN initiates NS-Block or NS-Unblock for the specified NSVC of the specified NSE:
  - *nsvc_id*: an integer from 0 through 65535.
  - *nse_id*: an integer from 0 through 65535.
- **reset nse-id** *nse_id* - SGSN initiates NS-Reset for all NSVC configured in the NSE. *nse_id* is an integer from 0 through 65535.
- **unblock nse-id** *nse_id* - SGSN initiates NS-Unblock for all NSVC configured for the specified NSE. *nse_id* is an integer from 0 through 65535.

sgsn-invoke-trace nse-id *nse_id* **record-type** *record_type* **trace-reference** *reference* **[mobile-id type** *id_type* **| trace-transaction-id** *trace_id* **]** :

Important This command can be used for troubleshooting/debugging purposes and is primarily intended for the use of specially trained service representatives.

Instructs the SGSN (1) to send the BSSGP message SGSN-INVOKE-TRACE to the BSC to initiate a BSC trace of a particular MS and (2) to define the type and triggering of the trace.

- *nse_id*: Identifies the peer NSE, enter an integer from 0 to 65535.
- *record_type*: Specifies the type of trace to be performed:
  - **basic**
  - **handover**
  - **no-bss-trace**
  - **radio**

- **trace-reference** *reference* : Specifies the trace reference ID as an integer from 0 to 65535.
- **mobile-id type** *id_type*: Select the appropriate mobile ID type for the MS that is to be traced:
  - **imei value** *value* - Specifies the mobile ID type as the unique International Mobile Equipment Identity.

    value: 15-digit IMEI value.
  - **imeisv value** *value*: Specifies the mobile ID type as the unique International Mobile Equipment Identity with the two-digit software version number.

    value: 16-digit IMEISV value.
  - **imsi value** *value* - Specifies the mobile ID type as a network unique International Mobile Subscriber Identity as a 15-digit IMSI value.
- **trace-transaction-id** *trace_id*: Specifies the trace transaction ID as an integer from 0 through 65535.

show plmn-list smgr-inst *sessmgr#*

Important This function is only available in release 8.1.

SGSN displays the configured PLMN list for the specified session manager (SessMgr):

sessmgr#: Enter up to 4 digits, 0 to 4095.

ss7-rd *ss7-rd_id* { destination | link | linkset | peer }

The **ss7-rd** commands assist with troubleshooting connections between the SGSN and the peer server.

ss7-rd_id: Specifies the configured SS7 routing domain as an integer from 1 through 12.

- **destination audit asp-instance** *asp_id* **peer-server-id** *peer_id* **psp-instance-id** *psp_id*

  Initiates destination audit (DAUD) messages for all point codes reachable via the identified peer-server, which is in restricted/unavailable/congested state due to DRST/DUNA/SCON messages respectively from the far end.
  - *asp_id*: Specifies the relevant ASP configuration ID as an integer from 1 through 4.
  - *peer_id*: Specifies the relevant peer server configuration ID as an integer from 1 through 144.
  - *psp_id*: Specifies the relevant PSP configuration ID as an integer from 1 through 4
- **link** *procedure* **linkset-id** *linkset_id* **link-id** *link_id*

  Initiates MTP3 network link management procedures for the specified link:
  - **activate**: Activates the deactivated link.
  - **deactivate**: Deactivates specified link.
  - **deactivate-l2-only**: Deactivates the link only at the MTP3 layer.
  - **inhibit**: Inhibits the link only if it does *not* make any destination unreachable.

- **uninhibit**: Uninhibits the inhibited link.
- *linkset_id*: an integer between 1 and 144.
- *link_id*: an integer between 1 and 16.

- **linkset-id** *procedure* **linkset-id** *linkset_id*

  Initiates MTP3 network link management procedures for all the links in the specified linkset:
  - **activate**: Activates the deactivated linkset.
  - **deactivate**: Deactivates the linkset.
  - **deactivate-l2-only**: Deactivates the linkset only at MTP3 layer.
  - *linkset_id*: an integer between 1 and 144.

- **peer** *message* **asp-instance** *asp_id* **peer-server-id** *peer_id* **psp-instance-id** *psp_id*

  Initiates one of the following SCTP/M3UA management messages from the identified link:
  - **abort**: Sends an SCTP Abort message which aborts the SCTP association ungracefully.
  - **activate**: Sends an M3UA ASP Active message to activate the link.
  - **down**: Sends an M3UA ASP Down message to bring down the M3UA link.
  - **establish**: Sends an SCTP INIT message to start the SCTP association establishment.
  - **inactivate**: Sends an M3UA ASP Inactive message to deactivate the link.
  - **inhibit**: Inhibits the M3UA link locally when the operator wants to lockout the link.
  - **terminate**: Sends SCTP Shutdown message which closes the SCTP association gracefully.
  - **un-inhibit**: Uninhibits the M3UA link.
  - **up**: Sends an M3UA ASP UP message to bring up the M3UA link.
  - *asp_id*: Specifies a relevant ASP configuration ID as an integer from 1 through 4.
  - *peer_id*: Specifies the relevant peer server configuration ID as an integer from 1 through 144.
  - *psp_id*: Specifies the relevant PSP configuration ID as an integer from 1 through 4

Usage Guidelines

In most cases, an operator will block/unblock/reset from the BSC-side. The **nse** commands cause the SGSN to initiate actions, usually for one of the following reasons:

- to resolve issues on the BSC-side,
- as part of an upgrade to the BSC,
- as part of link expansion,
- to resolve NSVC/BVC status mismatches observed between the SGSN and BSC.

The **sgsn-invoke-trace** command initiates the trace procedure where the BSC begins a trace record on a specified MS.

Example

The following command instructs the SGSN to initiate an NS-Block for all NSVC associated with Frame Relay NSE ID *2422*:

```
sgsn op nse fr unblock nse-id 2422
```

Activate linkset *1* configured in SS7 routing domain *1*:

```
sgsn op ss7-rd 1 linkset activate linkset-id 1
```

sgsn retry-unavailable-ggsn

Marks the GGSN as available for further activation.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

sgsn retry-unavailable-ggsn *ip_address*

ip_address

Specifies the IP address of a GGSN in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Usage Guidelines

This command allows the operator to directly inform both the session manager and the SGTPC manager that the GGSN has been removed from a blacklist and is now available for activations. This action would override the GGSN blacklist timer configuration with **ggsn-fail-retry-timer** in the SGTP service configuration mode.

Example

The following command indicates that the GGSN identified by its IP address is now available for activation:

```
sgsn retry-unavailable-ggsn 209.165.200.232
```

sgsn trigger-congestion

This command triggers a congestion state for the entire SGSN for operations and maintenance purposes (e.g., testing).

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`sgsn trigger-congestion level { critical | major | minor }`

critical | major | minor

Select one of the three congestion severity levels. Each level is associated with congestion threshold settings and a congestion-action-profile.

Usage Guidelines

Use the **sgsn clear congestion** to disable congestion simulation and return to normal operations.

Use the **show congestion-control configuration** command to display the SGSN's congestion-control policy with the congestion-action-profile name association with the level of congestion severity.

Example

Enable critical congestion control response testing with th following command:

`sgsn trigger-congestion level critical`

sgtpc test echo sgsn-address

Initiates SGTPC echo test procedure.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`sgtpc test echo sgsn-address` *`sgsn_ip_address`* **`{ all | ggsn-address`** *`ggsn_ip_address`* **`}`**

sgsn-address *sgsn_ip_address*

Identifies the IP address of the SGSN issuing the test in IPv4 dotted-decimal notation.

all

Sends GTPC echo requests to all GGSNs having current sessions with the SGTP service.

ggsn-address *ggsn_ip_address*

Sends a GTPC echo request to the specified GGSN whether or not the GGSN has active sessions with the SGTP service. *ggsn_ip_address*is entered using IPv4 dotted-decimal notation.

Usage Guidelines

This command initiates a test for the GTPC echo procedure -- echo from the specified SGSN to a specified GGSN or to all GGSNs that have sessions with the SGTP service. Issue the command from the Exec Mode within the context in which the SGTP service is configured.

Note that if the GGSN does not respond to the initial echo request, the echo requests will be retried for the max-retransmissions times.

Example

This SGSN with IP address of *209.165.200.225* sends an echo test to all GGSNs attached to the SGTP service:

```
sgtpc test echo sgsn-address 209.165.200.225 all
```

shutdown

Terminates all processes within the chassis. After all processes are terminated, the system initiates a hardware reset (reboot). This command is identical to the **reload** command.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
shutdown [ ignore-locks ] [ -noconfirm ]
```

ignore-locks

Reboots the system regardless of any save configuration operations that may be currently running. StarOS displays a warning message but does not wait for save configuration requests to complete before initiating the reboot.

```
Warning: One or more other administrators are saving configuration
```

Caution Use of the **ignore-locks** keyword may result in file corruption.

-noconfirm

Executes the command without any additional prompts or confirmation from the user.

Usage Guidelines

The system performs a hardware reset and reloads the highest priority boot image and configuration file specified in the boot.sys file. Refer to the **boot system priority** command in the Global Configuration Mode for additional information on configuring boot images, configuration files and priorities.

By default (without the **ignore-locks** option specified) **shutdown** waits for save configuration operations to complete before initiating the reboot.

Important To avoid the abrupt termination of subscriber sessions, it is recommended that a new call policy be configured and executed prior to invoking the **shutdown** command. This policy sets busy-out conditions for the system and allows active sessions to terminate gracefully. Refer to the **newcall** command in the Exec Mode for additional information.

Caution Issuing this command causes the system to become unavailable for session processing until the reboot process is complete.

Example

The following command performs a hardware reset on the system:

```
shutdown
```

sleep

Pauses the command line interface (CLI).

Product

All

Privprivilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

sleep *seconds*

sleep *seconds*

Specifies the number of seconds to pause as an integer from 1 through 3600.

Usage Guidelines

Sleep is a command delay which is only useful when creating command line interface scripts such as predefined configuration files/scripts.

Example

The following will cause the CLI to pause for *30* seconds.

```
sleep 30
```

srp disable

Disables the sending of a NACK from a standby ICSR chassis.

Product

All products that support ICSR

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

srp disable nack micro-chkpt-cmd *chkpt_number* **[-noconfirm]**

chkpt_number

Specifies the checkpoint number to be disabled as an integer from 1 through 255. You can obtain checkpoint numbers (CMD ID) via the output of the **show srp checkpoint info** command.

-noconfirm

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

Usage Guidelines

Use this command to disable the sending of NACK messages from the standby chassis that trigger a full checkpoint from the active chassis. Sending full checkpoints increases SRP bandwidth. This command disables the NACK feature for a specific micro-checkpoint which is failing continuously.

You can re-enable the micro-checkpoint using the **srp enable nack micro-chkpt-cmd** command.

Example

The following command disables CMD ID 9 (SESS_UCHKPT_CMD_UPDATE_L2TPLNSSTATS).

```
srp disable nack micro-chkpt-cmd 9
```

srp enable

Enables the sending of a previously disabled NACK from a standby ICSR chassis.

Product

All products that support ICSR

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

srp enable nack micro-chkpt-cmd *chkpt_number* **[-noconfirm]**

chkpt_number

Specifies the checkpoint number to be enabled as an integer from 1 through 255. You can obtain checkpoint numbers (CMD ID) via output of the **show srp checkpoint info** command.

-noconfirm

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

Usage Guidelines

Use this command to enable the sending of previously disabled NACK messages from the standby chassis. This command enables the NACK feature for a specific micro-checkpoint.

You can disable a micro-checkpoint using the **srp disable nack micro-chkpt-cmd** command.

Example

The following command enables CMD ID 9 (SESS_UCHKPT_CMD_UPDATE_L2TPLNSSTATS).

```
srp enable nack micro-chkpt-cmd 9
```

srp initiate-audit

Initiates an SRP audit between active and standby ICSR chassis.

Product

All products that support ICSR

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

srp initiate-audit manual-with-sync

Usage Guidelines

When issued from the active chassis, this command initiates a forced audit between ICSR chassis. This audit ensures that two ICSR peers are synchronized and identifies any discrepancies prior to scheduled or unscheduled switchover events.

Example

The following command initiates a forced audit between ICSR chassis.

```
srp initiate-audit manual-with-sync
```

srp initiate-switchover

Changes the device status on the primary and backup chassis configured for Interchassis Session Recovery (ICSR) support employing Service Redundancy Protocol (SRP).

Product

All products that support ICSR

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`srp initiate-switchover [ force | post-processing-timeout | reset-route-modifier | timeout` *`seconds`* **`] [ -noconfirm ]`**

Important For release 20.0 and higher, ICSR will verify session manager connectivity on both chassis prior to allowing a manual switchover. If one or more of the session managers in the active chassis is not connected on the standby chassis, the switchover will not be initiated. An error message will appear on the screen noting the number of session managers that are mismatched. The **force** keyword can be used to initiate the switchover despite the mismatch(es). The output of the **show checkpoint statistics verbose** command will not indicate "Ready" for a session manager instance ("smgr inst") in the "peer conn" column for any instance that is not connected in the standby chassis.

force

Switchover by force, without any validating checks.

post-processing-timeout

Specifies the timeout value (in seconds) to initiate the post-switchover process as an integer from 0 through 3600.

reset-route-modifier

During a switchover, resets the route-modifier to the initial value.

timeout *seconds*

Specifies the number of seconds before a forced switchover occurs as an integer from 0 through 65535. Default: 300

-noconfirm

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

Usage Guidelines

This command executes a forced switchover from active to inactive. The command must be executed on the active system and switches the active chassis to the inactive state and the standby system to an active state.

The switchover will be blocked if one or more session managers are not connected on the standby chassis. The **force** keyword will initiate the switchover despite any session manager mismatches.

Example

The following initiates a switchover in *30* seconds.

```
srp initiate-switchover timeout 30
```

srp reset-auth-probe-fail

Resets Service Redundancy Protocol (SRP) authentication probe monitor failure information.

Product

All products that support Interchassis Session Recovery (ICSR)

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
srp reset-auth-probe-fail
```

Usage Guidelines

This command resets the auth probe monitor failure information to 0.

Example

The following command resets the auth probe monitor failure information to 0:

```
srp reset-auth-probe-fail
```

srp reset-diameter-fail

Resets Service Redundancy Protocol (SRP) Diameter monitor failure information.

Product

All products that support Interchassis Session Recovery (ICSR)

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
srp reset-diameter-fail
```

Usage Guidelines

This command resets the Diameter monitor failure information to 0.

Example

The following command resets the SRP Diameter monitor failure information:

```
srp reset-diameter-fail
```

srp reset-sx-fail

Resets the Service Redundancy Protocol (SRP) Sx monitor failure information.

Product

All products that support Interchassis Session Recovery (ICSR)

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
srp reset-diameter-fail
```

Usage Guidelines

This command resets the Sx monitor failure information.

srp terminate-post-process

Forcibly terminates post-switchover processing by primary and backup chassis configured for Interchassis Session Recovery (ICSR) support employing Service Redundancy Protocol (SRP).

Product

All products that support ICSR

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
srp terminate-post-process [ -noconfirm ]
```

-noconfirm

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

Usage Guidelines

Use this command to force the termination of post-switchover processing.

Example

```
srp terminate-post-process
```

srp validate-configuration

Initiates a configuration validation check from the active chassis via Service Redundancy Protocol (SRP).

Product

All products that support Interchassis Session Recovery (ICSR)

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`srp validate-configuration`

Usage Guidelines

Validates the configuration for an active chassis.

Example

The following command initiates a configuration validation check from the active chassis:

`srp validate configuraiton`

srp validate-switchover

Validates that both the active and standby chassis are ready for a planned Service Redundancy Protocol (SRP) switchover.

Product

All products that support Interchassis Session Recovery (ICSR)

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`srp validate-switchover`

Usage Guidelines

Validates that both the active and standby chassis are ready for a planned SRP switchover.

Example

The following example performs SRP readiness validation on both ICSR chassis:

`srp validate switchover`

ssh

Connects to a remote host using a secure shell (SSH) interface.

Product

All

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

ssh { *host_name* | *host_ip_address* } [**port** *port_num*] [**user** *user_name*]

host_name | host_ip_address

Identifies the remote node with which to attempt connection.

host_name: specifies the remote node using its logical host name which must be resolved via DNS lookup. This is an alphanumeric string of 1 through 127 characters.

host_ip_address: specifies the remote node using its assigned IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

port *port_num*

Specifies a specific port for connection as an integer from 1 through 65535. Default = 22

user *user_name*

Specifies the user name attempting connection as an alphanumerical string from 1 through 1024 characters.

Usage Guidelines

SSH connects to a remote network element using a secure interface.

Example

The following connects to remote host *remoteABC* as user *user1*.

```
ssh remoteABC user user1
```

The following connects to remote host *209.165.200.229* without any default user.

```
ssh 209.165.200.229
```

The following connects to remote host *209.165.200.229* via port *2047* without any default user.

```
ssh 209.165.200.229 port 2047
```

start crypto security-association

Initiates Internet Key Exchange (IKE) negotiations.

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

start crypto security-association *cryptomap*

cryptomap

Specifies the name of an existing crypto map policy to use when starting the IKE negotiations as an alphanumeric string of 1 through 127 characters.

Usage Guidelines

Use this command to start IKE negotiations for IPSec.

Example

The following command starts the IKE negotiations using the parameters set in the crypto map named *crytpomap1*:

start crypto security-association cryptomap1

statistics-collection

This command allows to dynamically enable collection of Charging, Firewall or Post-processing ruledef statistics.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

statistics-collection active-charging { { all | charging | firewall | post-processing } { callid *call_id* **| imsi** *imsi_number* **} }**
[no] statistics-collection active-charging { callid *call_id* **| imsi** *imsi_number* **}**

no

If previously configured, deletes the specified rule expression from the current ruledef.

all | charging | firewall | post-processing

- **all**: Specifies to collect all ruledef statistics.
- **charging**: Specifies to collect charging ruledef statistics.
- **firewall**: Specifies to collect firewall ruledef statistics.
- **post-processing**: Specifies to collect post-processing ruledef statistics.

callid *call_id*

Specifies a call identification number as an eight-byte hexadecimal number.

imsi *imsi_number*

Specifies the IMSI number to match.

imsi_number must be a sequence of digits.

Usage Guidelines

Use this command to dynamically enable collection of ruledef statistics — Charging, Firewall or Post-processing. By default, the statistics will not be maintained. If the command is not configured, statistics collection will not be enabled and the following error message will be displayed in the **show active-charging sessions full** CLI — "statistics collection disabled; not collecting <*charging/firewall/postprocessing*> ruledef stats".

Example

The following command will collect firewall ruledef statistics with call ID set to *004c9961*:

```
statistics-collection active-charging firewall callid 004c9961
```

system packet-dump

Initiates a packet dump on an SF or CF card in a VPC-DI system.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax Description

```
system packet-dump { di-net card slot_num | port service_port } [ bond { a |
 b } | direction { both-rxtx | rx | rxtx | tx } | duration seconds |
packet-type { ipv4 | ipv6 } | pcapfile-size  size  | pcapfile-split-val
value  | protocol { icmpv4 | icmpv6 | tcp | udp } | to file filename ]
```

di-net card *slot_num*

Specifies the card from 1 through *n*.

port *card_port/port_num*

Specifies the ethernet interface based on the card number from 1 through *n* and port number from 1 through 50, for example 3/1.

bond { a | b }

Specifies a slave for bonded interfaces.

direction { both-rxtx | rx | rxtx | tx }

Specifies a filter for the direction of the packets to capture, either receive (**rx**), transmit (**tx**), or both (**rxtx**). Use the **both-rxtx** option to capture both receive and transmit, but output each to separate files.

duration *seconds*

Specifies the number of seconds from 1 through 600 for the packet dump. Default: 5 seconds

packet-type { ipv4 | ipv6 }

Specifies a filter for the type of the packets to capture, either **ipv4** or **ipv6**.

pcapfile-size *size*

Specifies the maximum size for each packet capture (pcap) file from 10 to 800 megabytes. Default: 10 megabytes.

pcapfile-split-val *value*

Specifies the number of pcap files to generate for a given capture from 0 to 10. Default: 0 (do not split files).

protocol { icmpv4 | icmpv6 | tcp | udp }

Specifies a filter for the protocol of the packets to capture, either **icmpv4**, **icmpv6**, **tcp**, or **udp**.

to file { /flash | /hd-raid | /cdrom1 | /sftp } [/directory]/ *filename*

Specifies the output location and filename.

Usage Guidelines

Use this command to perform packet captures to troubleshoot issues within a VPC-DI deployment.

Example

The following command initiates a packet dump on card in slot 7, port 1, and output the dump to a file stored locally at /flash/example7-1.pcap

```
system packet-dump port 7/1 to file /flash/example7-1.pcap
```

system ping

Initiates a ping test on the internal network between two VMs within the VPC-DI system.

Product VPC-DI

Privilege Security Administrator, Administrator

Command Modes Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`system ping from card` *`slot_num`* **`to card`** *`slot_num`* **`[ count`** *`number_of_packets`* **`| size`** *`bytes`* **`]`**

from card *slot_num*

Specifies the card slot number from 1 through *n* from which the ping test originates.

to card *slot_num*

Specifies the destination card slot number from 1 through *n*.

count *number_of_packets*

Sets the number of ping packets from 1 through 10000 to be sent. Default: 5 packets

size *bytes*

Sets the size of the ICMP Datagram in bytes from 40 to 18432. Default: 56

Usage Guidelines Use this command to perform ping tests to troubleshoot connectivity issues within a VPC-DI deployment.

Example

The following command initiates a ping test of 1000 packets from the card in slot 1 to the card in slot 9:

```
system ping from card 1 to card 9 count 1000
```

system ssh

Manages the persistent ssh user keys used for the internal ssh sessions between cards (VMs) in a VPC-DI system.

Product VPC-DI

Privilege Security Administrator

Command Modes Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

system ssh key { copy boot1 to card *slot_num* **| create boot1 }**

no system ssh key boot1 { all | card *slot_num* **}**

no system ssh key boot1 { all | card *slot_num* }

Deletes the persistent ssh keys on a specific card or all cards in the VPC-DI system. Deletion of keys may be used to purge a VM of the persistent keys or prepare the system for using a different distribution method (ESC, OpenStack, attached ISO).

- **all** : Deletes the ssh keys on all cards in the VPC-DI system.
- **card** *slot_num* : Deletes the ssh keys on the card specified by *slot_num* .

Note This command does not affect the VM until it is rebooted. It will continue to use the active key found during its boot.

copy boot1 to card *slot_num*

Transfers the persistent ssh keys (both public and private) in /boot1 on the active CF to another VM. That VM must be in a state to accept it by a user with console access placing it in receiver mode during its failed boot.

create boot1

Creates new persistent ssh keys (both public and private) and stores it in /boot1 on the active CF.

Note This command does not affect the VM until it is rebooted. It will continue to use the active key found during its boot.

Usage Guidelines

Use this command to manage the internal ssh keypairs in a VPC-DI deployment. While StarOS provides sshd services for user CLI and SFTP sessions on the management VMs (CF), another set of sshd services run for the exlusive use of internal communication between all component VMs, such as for remote command execution and file transfers. This internal sshd is only used on the internal DI-network interface.

This command enables you to store and manage ssh keys on the VM's virtual hard disk drive (HDD). This provides an alternate option for storing ssh keypairs besides the other methods such as Cisco Elastic Services Controller (ESC), OpenStack, or a directly attached ISO. The /boot1 partition is only accessible by a security administrator.

Use the **show system ssh key status** command to display the fingerprint of the current public key in use, the origin of where the key was found, and the status of all online VMs.

Example

The following command copies the ssh keypairs from the active CF to the card in slot 12

```
system ssh key copy boot1 to card 12
```