

HSGW Service Configuration Mode Commands

The HSGW Service Configuration Mode is used to create and manage a configuration allowing the HRPD Serving Gateway (HSGW) to communicate, send and receive call data, and session flows to/from a evolved Access Network/evolved Packet Control Function (eAN/ePCF) in an eHRPD network.

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context *context_name* **> hsgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

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

- a11-signalling-packets, on page 2
- associate, on page 3
- bind address, on page 3
- context-retention-timer, on page 5
- data-available-indicator, on page 5
- data-over-signaling, on page 6
- dns-pgw, on page 6
- end, on page 8
- exit, on page 8
- fqdn, on page 8
- fragment, on page 10
- gre, on page 10
- ip, on page 13
- lifetime, on page 15
- max-retransmissions, on page 16
- mobile-access-gateway, on page 17
- network-initiated-qos, on page 17
- plmn id, on page 18
- policy overload, on page 19
- profile-id-qci-mapping, on page 20

- registration-deny, on page 21
- retransmission-timeout, on page 22
- rsvp, on page 23
- setup-timeout, on page 24
- spi remote-address, on page 25
- ue-initiated-qos, on page 27
- unauthorized-flows, on page 27

a11-signalling-packets

Enables the DSCP marking feature for IP headers carrying outgoing A11-signalling A11 packets (such as RRP, RU, SU).

Product

HSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context *context_name* **> hsgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

Syntax Description

a11-signalling-packets ip-header-dscp *value*
[default | no] a11-signalling-packets ip-header-dscp

default

Restores the specified parameter to its default setting of 0x0.

no

Disables the specified functionality.

ip-header-dscp *value*

Configures the QoS Differentiated Services Code Point (DSCP) marking for IP header encapsulation.

value: Represents the DSCP setting as the first six most-significant bits of the ToS field. It can be configured to any hex value from 0x0 through 0x3F. Default is 0x0.

Usage Guidelines

Use this command to enable or disable the DSCP marking feature for IP headers carrying outgoing A11-signalling A11 packets. DSCP marking is disabled by default.

Example

The following command configures the HSGW service to support DSCP marking for IP headers on A11 packets in outgoing A11-signalling traffic:

```
a11-signalling-packets ip-header-dscp 0x21
```

associate

Associates accounting policies and QCI-QoS mapping parameters with this HSGW service.

Product

HSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context *context_name* **> hsgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

Syntax Description

```
associate { accounting-policy name | qci-qos-mapping name }
no associate { accounting-policy [ name ] | qci-qos-mapping }
```

no

Removes the specified associated policy or mapping from the service.

accounting-policy *name*

Specifies an existing accounting policy to associate with the HSGW service as an alphanumeric string of 1 through 63 characters.

qci-qos-mapping *name*

Specifies an existing QCI-QoS mapping configuration as an alphanumeric string of 1 through 63 characters.

QCI-QoS mapping is configured through the **qci-qos-mapping** command in the Global Configuration Mode.

Usage Guidelines

Use this command to associate an accounting policy with the HSGW service.

Example

The following command associates an accounting policy named *acct2* to the HSGW service:

```
associate accounting-policy acct2
```

bind address

Binds the service to a logical IP interface serving as the A10 interface and specifies the maximum number of subscribers that can access this service over the configured interface.

Product

HSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context *context_name* **> hsgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

Syntax Description

```
bind address ip_address [ max-subscribers num ]
no bind address
```

no

Removes the interface binding from this service.

address *ip_address*

Specifies the IP address of the A10/A11 interface in IPv4 dotted-decimal notation.

max-subscribers *num*

Specifies the maximum number of subscribers that can access this service on this interface as an integer from 0 through 2500000. Default: 2500000



Important The maximum number of subscribers supported is dependant on the license key installed and the number of active PSCs in the system. A fully loaded system with 13 active PSCs can support 3,000,000 total subscribers. Refer to the license key command and the Usage section (below) for additional information.

Usage Guidelines

Associate the HSGW service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an A10/A11 interface that provides the session connectivity to/from an eAN/PCF. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.

This command also sets a limit as to the number of simultaneous subscribers sessions that can be facilitated by the service/interface at any given time.

When configuring the **max-subscribers** option, be sure to consider the following:

- The total number of A10/A11 interfaces you will configure
- The total number of subscriber sessions that all of the configured interfaces may handle during peak busy hours
- An average bandwidth per session multiplied by the total number of sessions
- The type of physical port (10/100Base-T or 1000Base-Tx) that these interfaces will be bound to

Taking these factors into account and distributing your subscriber session across all available interfaces will allow you to configure your interfaces to optimally handle sessions without degraded performance.

Example

The following command would bind the logical IP interface with the address of *209.165.200.248* to the HSGW service and specifies that a maximum of *200,000* simultaneous subscriber sessions can be facilitated by the interface/service at any given time:

```
bind address 209.165.200.248 max-subscribers 200000
```

context-retention-timer

Configures the maximum number of consecutive seconds that a UE session context (which includes the LCP, authentication and A10 session context for a given UE) is maintained by the HSGW before it is torn down.

Product

HSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context *context_name* **> hsgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

Syntax Description

context-retention-timer timeout [*sec* **]**
[default | no] context-retention-timer timeout

default

Disables the timer.

no

Disables the timer.

timeout [*sec*]

Specifies the amount of time (in seconds) that the session context is maintained before it is disassembled as an integer from 1 through 3600. Default: 60.

In Release 15.0 and later, the maximum value has been increased to 86400 seconds (24 hours).

Usage Guidelines

Use this command to configure a timer to retain session contexts for a specified amount of time before disassembling it.

Example

The following command allows the HSGW to maintain session contexts for *120* seconds before tearing them down:

```
context-retention-timer timeout 120
```

data-available-indicator

Enables sending the Data Available Indicator extension in A10/A11 Registration Reply messages.

Product HSGW

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context *context_name* **> hsgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

Syntax Description **data-available-indicator**

Usage Guidelines Use this command to enable the sending of the Data Available Indicator extension in A10/A11 Registration Reply messages.

data-over-signaling

Enables the data-over-signaling marking feature for A10 packets.

Product HSGW

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context *context_name* **> hsgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

Syntax Description **[default | no] data-over-signaling**

default

Enables the data-over signaling feature for A10 packets.

no

Disables the data-over signaling feature for A10 packets.

Usage Guidelines Use this command to enable or disable the data-over signaling feature for A10 packets.

dns-pgw

Identifies the location of the DNS client to the HSGW service and enables/disables P-GW load balancing using DNS SRV lookup.

Product HSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context *context_name* **> hsgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

Syntax Description

dns-pgw { context *name* **| selection { topology [weight] | weight } } [default | no] dns-pgw { context | selection { topology [weight] | weight } }**

default

Returns the command to its default setting of the current context.

By default, topology will be enabled and weight will be disabled.

no

Removes the configured DNS client context name or P-GW DNS selection criteria from this service.

context *name*

Specifies an existing context in which the DNS client is configured as an alphanumeric string of 1 through 79 characters.

selection { topology [weight] | weight }

Specifies P-GW DNS selection criteria.

topology: Enables topology selection, which selects a P-GW topologically closer to the HSGW.

topology weight: Enables topology selection with weight.

weight: Enables selection with weight only when both preference values are the same; disables topology selection.

Usage Guidelines

Use this command to identify to the HSGW service the context where the DNS client is configured. The DNS client is used to identify an FQDN for the peer P-GW. This command defaults to the same context as the HSGW service.

In addition, this command enables and disables P-GW load balancing using DNS SRV lookup by defining P-GW DNS selection criteria.

Example

The following command identifies the context where the DNS client is configured as *isp3*:

```
dns-pgw context isp3
```

The following command enables P-GW DNS topology selection with weight:

```
dns-pgw selection topology weight
```

end

Exits the current configuration mode and returns to the Exec mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description

```
end
```

Usage Guidelines Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description

```
exit
```

Usage Guidelines Use this command to return to the parent configuration mode.

fqdn

Configures the Fully Qualified Domain Name (FQDN) for this HSGW service.

Product HSGW

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context *context_name* **> hsgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

Syntax Description

```
fqdn domain_name
[ default | no ] fqdn
```

default

Returns the command to the default setting of "null".

no

Removes the configured FQDN name from this service.

domain_name

Specifies an FQDN for the HSGW service as an alphanumeric string of 1 through 256 characters.



Important In order to properly interact with other nodes in the network, the FQDN should be 96 alpha and/or numeric characters or less.

Usage Guidelines

Use this command to configure an FQDN for this HSGW service. The FQDN is used when matching a P-GW with an HSGW.

Topology Matching

You may specify which P-GW you wish an HSGW interface to connect with by enabling topology matching within the FQDNs for both the HSGW service and P-GW service. Topology matching selects geographically closer nodes and reduces backhaul traffic for a specified interface.

The following optional keywords enable or disable topology matching when added to the beginning of an FQDN:

- **topon**.<*interface_name*>.

  Beginning an FQDN with **topon** initiates topology matching with available P-GWs in the network. Once this feature is enabled, the rest of the FQDN is processed from right to left until a matching regional designator is found on a corresponding P-GW FQDN.

- **topoff**.<*interface_name*>.

  By default, topology matching is disabled. If you enable topology matching for any interfaces within a node, however, all interfaces not using this feature should be designated with **topoff**.

Example

The following command configures this HSGW service with an FQDN of *abc123.com*:

```
fqdn abc123.com
```

The following command configures this HSGW service with an FQDN that enables topology matching:

```
fqdn topon.<interface_name>.hsgw01.bos.ma.node.epc.mnc<value>.
mcc<value>.3gppnetwork.org
```



Important The associated P-GW service must have a corresponding FQDN similar to the following:

```
topon.<interface_name>.pgw01.bos.ma.node.epc.mnc<value>.mcc<value>.3gppnetwork.org
```

fragment

Enables or disables Point-to-Point Protocol (PPP) payload fragmentation.

Product HSGW

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context *context_name* **> hsgw-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-hsgw-service)#`

Syntax Description **[default | no] fragment ppp-data**

default

Returns the command to its default setting of enabled.

no

Disables PPP payload fragmentation.

Usage Guidelines Use this command to enable or disable PPP payload fragmentation.

gre

Configures Generic Routing Encapsulation (GRE) parameters for the A10 protocol within the HSGW service.

Product HSGW

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context *context_name* **> hsgw-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-hsgw-service)#`

Syntax Description
```
gre { checksum | checksum-verify | flow control [ action {
disconnect-session | resume-session } ] [ timeout msecs ] + | ip-header-dscp
 value { all-control-packets | setup-packets-only } | reorder-timeout msecs
 | segmentation | sequence-mode { none | reorder } | sequence-numbers |
threegppp2-ext-headers qos-marking }
default gre { checksum | checksum-verify | flow-control | ip-header-dscp
 | reorder-timeout | sequence-mode | sequence-numbers |
threegppp2-ext-headers qos-marking }
```

no gre { checksum | checksum-verify | flow-control | ip-header-dscp | segmentation | sequence-numbers | threegppp2-ext-headers qos-marking }

default

Restores the specified parameter to its default setting.

no

Disables the specified functionality.

checksum

Enables the introduction of the checksum field in outgoing GRE packets. Default: disabled

checksum-verify

Enables verification of the GRE checksum (if present) in incoming GRE packets. Default: disabled

flow-control [action { disconnect-session | resume-session }] [timeout *msecs*] +

Default: no GRE flow-control

Enables 3GPP2 GRE flow control which causes the HSGW to send flow control enabled Normal Vendor Specific Extensions (NVSE) in A11 RRPs.

action { disconnect-session | resume-session }:

Default: disconnect-session

Specifies the action to be taken when timeout is reached:

- **disconnect-session**: Ends the session and releases the call.
- **resume-session**: Switches flow control to XON and resumes delivery of packets to the RAN.

timeout *msecs*

Specifies the amount of time (in milliseconds) to wait for an XON indicator from the RAN (after receiving an XOFF). Also sets the action to be taken if the timeout limit is reached.

msecs is an integer from 1 through 1000000. Default: 1000

ip-header-dscp *value* { all-control-packets | setup-packets-only }

Default: Disabled

Configures QoS Differentiated Services Code Point (DSCP) marking for GRE packets.

- *value*: Represents the DSCP setting as the first six most-significant bits of the ToS field. It can be configured to any hexadecimal value from 0x0 through 0x3F.
- **all-control-packets**: Dictates that the DSCP marking is to be provided in all GRE control packets.
- **setup-packets-only**: Dictates that the DSCP marking is to be provided only in GRE setup packets.

reorder-timeout *msecs*

Configures the maximum number of milliseconds to wait before processing reordered out-of-sequence GRE packets as an integer from 0 through 5000. Default: 100

segmentation

Enables GRE Segmentation for the HSGW service. Default: disabled

sequence-mode { none | reorder }

Default: none

Configures handling of incoming out-of-sequence GRE packets.

none: Specifies that sequence numbers in packets are ignored and all arriving packets are processed in the order they arrive.

reorder: Specifies that out of sequence packets are stored in a sequencing queue until one of the conditions is met:

- The reorder timeout occurs: All queued packets are sent for processing and the accepted sequence number is updated to the highest number in the queue.
- The queue is full (five packets): All packets in the queue are sent for processing, the reorder timer is stopped and the accepted sequence number is updated to the highest number in the queue.
- An arriving packet has a sequence number such that the difference between this and the packet at the head of the queue is greater than five. All the packets in the queue are sent for processing, the reorder timer is stopped and the accepted sequence number is updated to the highest number that arrived.
- A packet arrives that fills a gap in the sequenced numbers stored in the queue and creates a subset of packets whose sequence numbers are continuous with the current accepted sequence number. This subset of packets in the queue is sent for processing. The reorder timer continues to run and the accepted sequence number is updated to the highest number in the subset delivered.

sequence-numbers

Enables insertion of GRE sequence numbers in data that is about to be transmitted over the A10 interface. Data coming into the system containing sequence numbers but that is out of sequence is not re-sequenced.

threegppp2-ext-headers qos-marking

When threegppp2-ext-headers qos-marking is enabled and the PCF negotiates capability in the A11 RRQ, the HSGW will include the QoS optional data attribute in the GRE 3gpp2 extension header.

The **no** keyword, enables qos-marking in the GRE header based on the tos value in the header.

Usage Guidelines

Use this command to set GRE parameters for the A10 protocol within the HSGW service.

Example

The following command configures the HSGW service to support the inclusion of GRE sequence numbers in outgoing traffic:

```
gre sequence-numbers
```

ip

Enables the use of Robust Header Compression (RoHC) and enters the HSGW Service ROHC Configuration Mode where RoHC parameters are configured for the service.

Configures the local User Datagram Protocol (UDP) port for the A10/A11 interface IP socket.

Sets the parameters for IP source validation. Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network. Source validation requires the source address of received packets to match the IP address assigned to the subscriber (either statically or dynamically) during the session.

Product

HSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context *context_name* **> hsgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

Syntax Description

```
ip { header-compression rohc | local-port number | source-violation {
clear-on-valid-packet | drop-limit num | period secs | reneg-limit num } }
default ip { header-compression rohc | local-port | source-violation {
drop-limit | period | reneg-limit } }
no ip { header-compression rohc | source-violation clear-on-valid-packet
 }
```

default

Resets the keyword to its default value.

no

header-compression rohc: Removes the RoHC configuration from this service.

ip source-violation clear-on-valid-packet: Disables the ability of the service to reset the reneg-limit and drop-limit counters after receipt of a properly addressed packet.

header-compression rohc

Specifies that Robust Header Compression will be applied to sessions using this service and enters the HSGW Service RoHC Configuration Mode where RoHC parameters are configured.

local-port *number*

Specifies the UDP port number as an integer from 1 through 65535. Default: 699

source-violation { clear-on-valid-packet | drop-limit *num* | period *secs* | reneg-limit *num* }

clear-on-valid-packet

Configures the service to reset the reneg-limit and drop-limit counters after receipt of a properly addressed packet. Default: disabled

drop-limit *num*

Specifies the number of allowed source violations within a detection period before forcing a call disconnect as an integer from 1 through 1000000. If *num* is not specified, the value is set to the default. Default: 10

period *secs*

Specifies the length of time (in seconds) for a source violation detection period to last; drop-limit and reneg-limit counters are decremented each time this value is reached.

The counters are decremented in this manner: reneg-limit counter is reduced by one (1) each time the period value is reached until the counter is zero (0); drop-limit counter is halved each time the period value is reached until the counter is zero (0). If *secs* is not specified, the value is set to the default.

secs is an integer from 1 through1000000. Default: 120

reneg-limit *num*

Sets the number of allowed source violations within a detection period before forcing a PPP renegotiation. If *num* is not specified, the value is set to the default.

num is an integer from 1 through 1000000. Default: 5

Usage Guidelines

Header Compression RoHC: Use this command to specify that sessions using this service will have Robust Header Compression applied and configure parameters supporting RoHC.

Entering this command results in the following prompt:

```
[context_name]hostname(config-ip-header-compression-rohc)#
```

HSGW Service RoHC Configuration Mode commands are defined in the HSGW Service RoHC Configuration Mode Commands chapter.

Local Port: Specify the UDP port that should be used for communications between the Packet Control Function (PCF) and the HSGW.



Important The UDP port setting on the PCF must match the local-port setting for the HSGW service on the system in order for the two devices to communicate.

Source Violation: This function is intended to allow the operator to configure a network to prevent problems such as when a user gets handed back and forth between two HSGWs a number of times during a handoff scenario.

This function operates in the following manner:

When a subscriber packet is received with a source address violation, the system increments both the IP source-violation reneg-limit and drop-limit counters and starts the timer for the IP-source violation period. Every subsequent packet received with a bad source address during the IP-source violation period causes the reneg-limit and drop-limit counters to increment.

For example, if reneg-limit is set to 5, then the system allows 5 packets with a bad source address (source violations), but on the 5th packet, it re-negotiates PPP.

If the drop-limit is set to 10, the above process of receiving 5 source violations and renegotiating PPP occurs only once. After the second 5 source violations, the call is dropped. The period timer continues to count throughout this process.

If the configured source-violation period is exceeded at any time before the call is dropped, the reneg-limit counter is checked. If the reneg-limit counter is greater than zero (0), the reneg-limit is decremented by 1. If the reneg-limit counter equals zero, the drop-limit is decremented by half.

Example

The following command specifies a UDP port of 3950 for the HSGW service to use to communicate with the PCF on the A10/A11 interface:

```
ip local-port 3950
```

The following command sets the drop limit to *15* and leaves the other values at their defaults:

```
ip source-violation drop-limit 15
```

lifetime

Specifies how long an A10 connection can exist before its registration is considered expired.

Product

HSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > **context** *context_name* > **hsgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

Syntax Description

lifetime *time*
[default | no] lifetime

default

Resets the lifetime value to the default setting of 1800 seconds.

no

Specifies that an A10 connection can exist for an infinite amount of time.

time

Specifies the time (in seconds) that an A10 connection can exist before its registration is considered expired as an integer from 1 through 65534. Default: 1800

Usage Guidelines Use this command to set a limit to the amount of time that a subscriber session can remain up whether or not the session is active or dormant. If the lifetime timer expires before the subscriber terminates the session, the connection is terminated automatically.

Example

The following command specifies a time of *3600* seconds (1 hour) for subscriber sessions on this HSGW service:

```
lifetime 3600
```

max-retransmissions

Configures the maximum number of times the HSGW service will attempt to communicate with an eAN/PCF before it marks it as unreachable.

Product HSGW

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context *context_name* **> hsgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

Syntax Description

```
max-retransmissions count
default max-retransmissions
```

default

Resets the maximum number of allowed retransmissions to the default value of 5.

count

Specifies the maximum number of times the HSGW service will attempt to communicate with an eAN/PCF before it marks it as unreachable.

count is an integer from 1 through 1000000. Default: 5

Usage Guidelines Use this command to limit the number of retransmissions to an eAN/PCF before marking it as unreachable. If the value configured is reached, the call is dropped.

Example

The following command configures the maximum number of retransmissions for the HSGW service to *3*:

```
max-retransmissions 3
```

mobile-access-gateway

Identifies the mobile access gateway (MAG) context through which MIPv6 calls are to be routed.

Product

HSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context *context_name* **> hsgw-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-hsgw-service)#`

Syntax Description

`mobile-access-gateway context` *`context_name`* **`[ mag-service`** *`service_name`* **`]`**
`no mobile-access-gateway context`

no

Removes the configured MAG context route from this service.

context *context_name* [mag-service *service_name*]

Specifies the name of the context and, optionally, the service through which MIPv6 sessions are to be routed.

context_name is an existing context expressed as an alphanumeric string of 1 through 79 characters.

service_name is an existing MAG service expressed as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to specify where MIPv6 sessions are routed through this service.

Example

The following command identifies the MAG context *MAG1* as the context through which MIPv6 sessions are to be routed and further narrows the route by specifying the service name (*mag_serv3*):

```
mobile-access-gateway context MAG1 mag-service mag_serv3
```

network-initiated-qos

Enables the use of network initiated QoS functionality.

Product

HSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context *context_name* **> hsgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

Syntax Description

```
[ default | no ] network-initiated-qos
```

default

Returns the command to its default setting of enabled.

no

Disables the ability to use network initiated QoS functionality.

Usage Guidelines

Use this command to enable or disable support for network initiated QoS functionality. Network initiated QoS is enabled by default.

When network initiated QoS functionality is enabled, if the vendor specific network control protocol (VSNCP) protocol configuration options (PCO) arrive from the UE with the BCM set, the HSGW CCR-I includes the Network-Request-Support AVP. If the PCRF behavior returns a BCM of MS+NW when this AVP is received, then flows originating from the network (RSVP Resv) would be triggered upon a PCC-Rule install.

plmn id

Configures Public Land Mobile Network identifiers used to determine if a mobile station is visiting, roaming or belongs to this network.

Product

HSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context *context_name* **> hsgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

Syntax Description

plmn id mcc *number* **mnc** *number*

mcc *number* mnc *number*

mcc *number*: Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer fromn 100 through 999.

mnc *number*: Specifies the mobile network code (MNC) portion of the PLMN identifier as a 2- or 3-digit integer from 00 through 999.

Usage Guidelines

The PLMN identifier is used to aid the HSGW service in the determination of whether or not a mobile station is visiting, roaming, or home. Multiple P-GW services can be configured with the same PLMN identifier. Up to five PLMN IDs can be configured for each P-GW Service. The configured IDs are used in Diameter-EAP-Request messages (as a Visited-Network-Identifier AVP).

Example

The following command configures the PLMN identifier with an MCC of *462* and MNC of *2*:

```
plmn id mcc 462 mnc 02
```

policy overload

Specifies how an HSGW service should handle overload conditions.

Product

HSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > **context** *context_name* > **hsgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

Syntax Description

```
policy overload { redirect address [ weight weight_num ] [ address2 [ weight
weight_num ] ... address16 [ weight weight_num ] ] | reject [ use reject-code
{ admin-prohibit | insufficient-resources } ] }
default policy overload
no policy overload [ redirect address [ address2 ] ... [ address16 ]
```

default

Returns the command to it default setting of "reject" with the "admin-prohibited" code.

no

Removes a specified "redirect address" from this service.

redirect *address* [weight *weight_num*] [*address2* [weight *weight_num*] ... *address16* [weight *weight_num*]]

This option enables a redirect policy for overloading conditions. When a redirect policy is invoked, the HSGW service rejects new sessions with an A11 Registration Reply Code of 88H (unknown HSGW address) and provides the IP address of an alternate HSGW. This command can be issued multiple times.

address: The IP address of an alternate HSGW 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 (default). *weight_num* must be an integer value from 1 through 10.

reject [use reject-code { admin-prohibite | insufficient-resources }]

This option will cause any overload traffic to be rejected. The HSGW sends an A11 Registration Reply Code of 82H (insufficient resources).

use-reject-code admin-prohibited: When this keyword is specified and traffic is rejected, the error code admin prohibited is returned instead of the error code "insufficient resources". This is the default behavior.

use-reject-code insufficient-resources: When this keyword is specified and traffic is rejected, the error code "insufficient resources" is returned instead of the error code admin prohibited.

Usage Guidelines

Policies can be implemented to dictate HSGW service behavior for overload conditions.

The system invokes the overload policy if the number of calls currently being processed exceeds the licensed limit for the maximum number of sessions supported by the system.

The system automatically invokes the overload policy when an on-line software upgrade is started.

Use the **no policy overload** command to delete a previously configured policy. If after deleting the policy setting you desire to return the policy parameter to its default setting, use the **default policy** command.

The chassis is shipped from the factory with the policy options overload disabled

Example

The following command configures the HSGW service to redirect overload traffic to two IPv4 addresses, one priority weighted *1* and the other priority weighted *5*:

```
policy overload redirect 209.165.200.229 weight 1 209.165.201.5 weight 5
```

profile-id-qci-mapping

Associates a configured mapping table for RP QoS Profile ID to LTE QoS Class Index (QCI) mapping with this service.

Product

HSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context *context_name* **> hsgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

Syntax Description

profile-id-qci-mapping *name*
no profile-id-qci-mapping [*name* **]**

no

Removes all profile maps or a specific profile map from this service.

name

Specifies the name of an existing Profile ID - QCI Mapping table to be associated with this service as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to associate the HSGW service with a configured Profile ID - QCI Mapping table. The table is configured in the Global Configuration Mode using the **profile-id-qci-mapping-table** command.

Example

The following command associates a Profile ID - QCI Mapping table named *table3* with this service:

```
profile-id-qci-mapping table3
```

registration-deny

Configures parameters related to registration rejection.

Product

HSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > **context** *context_name* > **hsgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

Syntax Description

```
registration-deny { handoff connection-setup-record-absent | newcall
connection-setup-record-absent } [ use-deny-code { poorly-formed-request
 | reason-unspecified } ]
[ default | no ] registration-deny { handoff connection-setup-record-absent
 | newcall connection-setup-record-absent }
```

default | no

Returns the command to its default settings.

handoff connection-setup-record-absent

When enabled, the HSGW denies or discards handoff R-P sessions that do not have an Airlink Connection Setup record in the A11 Registration Request.

Default is disabled. Default HSGW behavior is to accept such requests.

newcall connection-setup-record-absent

When enabled, the HSGW denies or discards new R-P sessions that do not have the Airlink Connection Setup record in the A11 Registration Request.

Default is disabled. Default HSGW behavior is to accept such requests.

use-deny-code { poorly-formed-request | reason-unspecified }

Sets the specified Registration Deny Code when denying a new call or handoff because of a missing connection setup record.

Usage Guidelines

Use this command to configure parameters relating to the rejection of registration requests.

Example

The following command denies registration for registration requests missing the connection setup record and replies with a use deny code of "poorly formed request":

```
registration-deny handoff connection-setup-record-absent use-deny-code
poorly-formed-request
```

retransmission-timeout

Configures the maximum allowable time for the HSGW service to wait for a response from the eAN/PCF before it attempts to communicate with the eAN/PCF again (if the system is configured to retry the PCF), or marks the eAN/PCF as unreachable.

Product

HSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context *context_name* **> hsgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

Syntax Description

retransmission-timeout *time*
[default | no] retransmission-timeout

default

Resets the timeout setting to the default value of 3.

no

Deletes a previously configured timeout value.

time

Specifies the maximum allowable time (in seconds) for the HSGW service to wait for a response from the eAN/PCF before it: a) attempts to communicate with the eAN/PCF again (if the system is configured to retry the PCF), or b) marks the eAN/PCF as unreachable.

time is an integer from 1 through 1000000. Default: 3

Usage Guidelines Use the retransmission timeout command in conjunction with the **max-retransmissions** command in order to configure the HSGW service's behavior when it does not receive a response from a particular PCF.

Example

The following command configures a retransmission timeout value of 5 seconds:

```
retransmission-timeout 5
```

rsvp

Configures resource reservation protocol (RSVP) parameters for this HSGW service in support of the network initiated QoS feature.

Product HSGW

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context *context_name* **> hsgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

Syntax Description

```
rsvp { max-retransmissions count | retransmission-timeout seconds }
[ default | no ] rsvp { max-retransmissions | retransmission-timeout }
```

default

Resets the maximum number of allowed retransmissions to the default value of 5 or the timeout setting to the default value of 3.

no

Disables the feature.

max-retransmissions *count*

Specifies the maximum retransmission count of RP control packets as an integer from 1 through 1000000. Default: 5

retransmission-timeout *seconds*

Specifies the maximum amount of time (in seconds) to allow for retransmission of RP control packets as an integer from 1 through 1000000. Default: 3

Usage Guidelines Use this command to set RSVP parameters for this HSGW service in support of the network initiated QoS feature.

Example

The following command configures the maximum number of retransmissions to *3*:

```
rsvp max-retransmissions 3
```

setup-timeout

Specifies the maximum amount of time allowed for session setup.

Product

HSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context *context_name* **> hsgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

Syntax Description

setup-timeout *seconds*
[default| no] setup-timeout

default

Resets the command to the default value of enabled with a timeout of 60 seconds.

no

Disables the feature.

seconds

Specifies the maximum amount of time (in seconds) to allow for setup of a session in this service as an integer from 1 though 1000000. Default: 60

Usage Guidelines

Use this command to set the maximum amount of time allowed for setting up a session.

Example

The following command sets the maximum time allowed for setting up a session to 5 minutes (300 seconds):

```
setup-timeout 300
```

spi remote-address

Configures the security parameter index (SPI) between the HSGW service and the evolved Access Network/evolved Packet Control Function (eAN/ePCF). This command also configures the redirection of calls based on the PCF zone.

Product

HSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context *context_name* **> hsgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

Syntax Description

```
spi remote-address { pcf_ip_address | ip_addr_mask_combo } spi-number number {
encrypted secret enc_secret | secret secret } [ description string ] [
hash-algorithm { md5 | rfc2002-md5 } ] [ replay-protection { nonce |
timestamp } ] [ timestamp-tolerance tolerance ] [ zone zone_id ]
no spi remote-address pcf_ip_address spi-number number
```

pcf_ip_address | ip_addr_mask_combo

pcf_ip_address: Specifies the IP address of the ePCF. *pcf_ip_address* is an IP address expressed in IPv4 dotted decimal notation or IPv6 colon separated notation.

ip_addr_mask_combo: Specifies the IP address and mask bits of the PCF. *ip_addr_mask_combo* must be specified using the form "IP Address/Mask Bits" where the IP address must in IPv4 dotted-decimal or IPv6 colon-separated notation, and the mask bits are a numeric value corresponding to the number of bits in the subnet mask.

spi-number *number*

Specifies the SPI which indicates a security context between the PCF and the HSGW as an integer from 256 through 4294967295.

encrypted secret *enc_secret* | secret *secret*

Configures the shared-secret between the HSGW service and the PCF. The secret can be either encrypted or non-encrypted.

encrypted secret *enc_secret*: Specifies the encrypted shared key (*enc_secret*) between the PCF and the HSGW service. *enc_secret* must be between 1 and 236 alpha and/or numeric characters and is case sensitive.

secret *secret*: Specifies the shared key (secret) between the PCF and the HSGW services. *secret* must be between 1 and 127 alpha and/or numeric characters and is case sensitive.

The **encrypted** keyword is intended only for use by the chassis while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **secret** keyword is the encrypted version of the plain text secret key. Only the encrypted secret key is saved as part of the configuration file.

description *string*

This is a description for the SPI expressed as an alphanumeric string of 1 through 31 characters.

hash-algorithm { md5 | rfc2002-md5 }

Specifies the hash-algorithm used between the HSGW service and the PCF. Default: md5

md5: Configures the hash-algorithm to implement MD5.

rfc2002-md5: Configures the hash-algorithm to implement keyed-MD5.

replay-protection { nonce | timestamp }

Specifies the replay-protection scheme that should be implemented by the HSGW service. Default: timestamp

nonce: Configures replay protection to be implemented using NONCE (Number ONCE).

timestamp: Configures replay protection to be implemented using timestamps.

timestamp-tolerance *tolerance*

Specifies the allowable difference (in seconds) between timestamps as an integer from 0 through 65535. If the difference is exceeded, the session will be rejected. If set to 0, timestamp tolerance checking is disabled at the receiving end. Default: 60

zone *zone_id*

Specifies the different PCF zones to configure in HSGW service. Mapping of a zone-number to a set of HSGWs can be done per HSGW service basis.

zone_id is an integer value from 1 through 32. A maximum of 32 PCF zones can be configured for a HSGW service.

Usage Guidelines

An SPI is a security mechanism configured and shared by the PCF and the HSGW service. Please refer to *IETF RFC 2002: IP Mobility Support* for additional information.

Multiple SPIs can be configured if the HSGW service is communicating with multiple eAN/ePCFs.



Important The SPI configuration on the PCF must match the SPI configuration for the HSGW service on the system in order for the two devices to communicate properly.

This command used with the **zone** keyword redirects all calls on the basis of PCF zone to the specific HSGW on the basis of parameters configured using the **policy pcf-zone-match** command.

Example

The following command configures the HSGW service to use an SPI of *256* when communicating with a PCF with the IP address *209.165.201.2*. The key that would be shared between the PCF and the HSGW service is *q397F65*.

```
spi remote-address 209.165.201.2 spi-number 256 secret q397F65
```

The following command creates the configured SPI of *400* for an PCF with an IP address of *209.165.202.128* and zone id as *11*:

```
spi remote-address 209.165.202.128 spi-number 400 zone 11
```

ue-initiated-qos

Configures the HSGW behavior for UE initiated QoS requests.

Product

HSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context *context_name* **> hsgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

Syntax Description

`[ default | no ] ue-initiated-qos`

default

Returns the HSGW to the default behavior, where UE initiated QoS requests are accepted and forwarded to the PCRF via Gxa interface.

no

Enables rejection of UE initiated QoS request for dedicated bearer in HSGW service. HSGW does not forward the request to the PCRF over Gxa and instead rejects the UE initiated QoS immediately.

Usage Guidelines

Use this command to enable or disable support for UE initiated QoS functionality.

By default, UE initiated QoS requests are accepted and forwarded to the PCRF via Gxa interface. If PCRF rejects the UE initiated QoS, UE request is rejected.

This command allows rejection of UE initiated QoS request for dedicated bearer in HSGW service. HSGW does not forward the request to the PCRF over Gxa and instead rejects the UE initiated QoS immediately.

Example

The following command rejects UE-initiated QoS request for dedicated bearer in HSGW service:

no ue-initiated-qos

unauthorized-flows

Configures the service to wait a specified number of seconds before triggering a QoS update to downgrade an unauthorized flow.

Product

HSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context *context_name* **> hsgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

Syntax Description

unauthorized-flows qos-update wait-timeout *seconds*
[default | no] unauthorized-flows qos-update wait-timeout

default

Returns the command to its default setting.

no

Removes the configure wait-timeout setting for this service.

qos-update wait-timeout *seconds*

Specifies the number of seconds to wait before triggering the QoS update to downgrade the unauthorized flow as an integer from 1 through 65534.

Usage Guidelines

Use this command to specific a wait timeout trigger for flows that are unauthorized by policy rules received via the Gxa interface from the PCRF. When the wit timer expires, the HSGW triggers a QoS update to downgrade the unauthorized flow.

Example

The following command configures the HSGW service to apply the wait time of *30* seconds after receiving an flow unauthorized by the PCRF:

```
unauthorized-flow qos-update wait-timeout 30
```