

Subscriber Configuration Mode Commands

The Subscriber Configuration Mode is used to create local subscribers as well as to set default subscriber options for the current context.

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-subscriber)#`

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

- aaa, on page 4
- access-link ip-fragmentation, on page 6
- accounting-mode, on page 7
- active-charging bandwidth-policy, on page 8
- active-charging link-monitor tcp, on page 9
- active-charging radio-congestion, on page 10
- active-charging rulebase, on page 11
- always-on, on page 12
- asn-header-compression-rohc, on page 13
- asn nspid, on page 14
- asn-pdfid, on page 15
- asn-policy, on page 16
- associate accounting-policy, on page 18
- authorized-flow-profile-id, on page 19
- content-filtering category, on page 20
- credit-control-client, on page 21
- credit-control-group, on page 22
- credit-control-service, on page 23
- data-tunneling ignore df-bit, on page 24
- dcca peer-select, on page 24
- default, on page 25

- description, on page 28
- dhcp dhcpv6, on page 29
- dhcp options, on page 30
- dhcp parameter-request-list-option, on page 30
- dhcp service, on page 31
- dns, on page 32
- do show, on page 33
- eap, on page 33
- encrypted password, on page 35
- end, on page 35
- exit, on page 35
- external-inline-server, on page 36
- firewall policy, on page 36
- fw-and-nat policy, on page 37
- gtpp, on page 38
- idle-timeout-activity, on page 39
- ikev2 tsr, on page 40
- ims application-manager, on page 41
- ims-auth-service, on page 42
- inter-pdsn-handoff, on page 43
- ip access-group, on page 43
- ip address, on page 44
- ip address alloc-method, on page 45
- ip address pool, on page 47
- ip address secondary-pool, on page 48
- ip allowed-dscp, on page 49
- ip context-name, on page 52
- ip header-compression, on page 53
- ip hide-service-address, on page 55
- ip local-address, on page 56
- ip multicast discard, on page 57
- ip qos-dscp, on page 57
- ip route, on page 59
- ip source-validation, on page 60
- ip user-datagram-tos copy, on page 60
- ip vlan, on page 62
- ipv6 access-group, on page 63
- ipv6 address, on page 63
- ipv6 dns, on page 64
- ipv6 dns-proxy, on page 65
- ipv6 egress-address-filtering, on page 66
- ipv6 initial-router-advt, on page 67
- ipv6 interface-id, on page 68
- ipv6 minimum-link-mtu, on page 69
- ipv6 secondary-address, on page 70
- l2tp send accounting-correlation-info, on page 71

- l3-to-l2-tunnel address-policy, on page 72
- loadbalance-tunnel-peers, on page 73
- long-duration-action, on page 74
- max-pdn-connections, on page 75
- mediation-device, on page 76
- mobile-ip, on page 77
- mobile-ip ha, on page 80
- mobile-ip reg-lifetime-override, on page 81
- mobile-ip send access-technology, on page 82
- mobile-ip send accounting-correlation-info, on page 83
- mobile-ip send bsid, on page 84
- mobile-ip send pcf-address, on page 85
- mobile-ip send service-option, on page 86
- mobile-ip send subnet-id, on page 87
- mobile-ipv6, on page 87
- nai-construction-domain, on page 89
- nbns, on page 89
- nexthop-forwarding-address, on page 90
- npu qos, on page 91
- nw-reachability-server, on page 92
- outbound, on page 93
- overload-disconnect, on page 94
- password, on page 95
- pdif mobile-ip, on page 97
- permission, on page 98
- policy ipv6 tunnel, on page 98
- policy-group, on page 99
- ppp, on page 100
- prepaid 3gpp2, on page 103
- prepaid custom, on page 105
- prepaid unclassify, on page 106
- prepaid voice-push, on page 107
- prepaid wimax, on page 107
- proxy-dns intercept list-name, on page 107
- proxy-mip, on page 108
- qos apn-ambr, on page 109
- qos rate-limit, on page 110
- qos traffic-police, on page 117
- qos traffic-shape, on page 119
- radius accounting, on page 122
- radius group, on page 124
- radius returned-framed-ip-address, on page 125
- radius rulebase-format, on page 126
- rohc-profile-name, on page 128
- secondary ip pool, on page 128
- send-destination-pgw, on page 129

- service-option, on page 130
- simultaneous, on page 131
- timeout absolute, on page 132
- timeout idle, on page 132
- timeout long-duration, on page 134
- tpo policy, on page 135
- tunnel address-policy, on page 135
- tunnel gre, on page 136
- tunnel ipip, on page 137
- tunnel ipsec, on page 138
- tunnel l2tp, on page 139
- w-apn, on page 141

aaa

Configures authentication, authorization and accounting (AAA) functionality at the subscriber level.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

```
[ no ] aaa { accounting interim { interval-timeout interval_timeout | normal
 | suppress } | group aaa_group_name | secondary-group aaa_secondary_group_name
}
default aaa { accounting interim [ interval-timeout ] | group |
secondary-group }
no aaa { accounting interim [ interval-timeout ] | group [ aaa_group_name ]
 | secondary-group }
```

default

Configures the default setting for the specified parameter.

- **accounting**: Enables AAA accounting for subscribers.
- **group**: Uses the default AAA group—the one specified at the context level or in the default subscriber profile.
- **secondary-group**: Removes the secondary AAA group from the subscriber configuration.

no

- **accounting**: Disables AAA accounting for subscribers.

- **group**: Uses the default AAA group—the one specified at the context level or in the default subscriber profile.
- **secondary-group**: Removes the secondary AAA group from the subscriber configuration.

accounting interim { interval-timeout *interval_timeout* | normal | suppress }

Specifies when system should send an interim accounting record to the server.

- **interval-timeout**: Specifies the time interval (in seconds) at which to send an interim accounting record.

  interval_timeout must be an integer from 50 through 40000000.
- **normal**: If RADIUS accounting is enabled, send this Acct-Status-Type message when normally required by operation.
- **suppress**: If RADIUS accounting is enabled, suppress the sending of Acct-Status-Type message.

group *aaa_group_name*

Specifies the AAA server group for the subscriber for authentication and/or accounting.

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

secondary-group *aaa_secondary_group_name*

Specifies the secondary AAA server group for the subscriber.

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

Usage Guidelines

Use this command to configure AAA functionality at the subscriber level.

Instead of having a single list of servers per context, this feature configures multiple server groups within a context and applies individual server group for subscribers in that context. Each server group consists of a list of AAA servers for each AAA function (accounting, authentication, charging, etc.).

The AAA secondary server group supports the No-ACK RADIUS Targets feature in conjunction with PDSN/HA for secondary accounting (with different RADIUS accounting group configuration) to the RADIUS servers without expecting the acknowledgement from the server, in addition to standard RADIUS accounting. This secondary accounting will be an exact copy of all the standard RADIUS accounting message (RADIUS Start/Interim/Stop) sent to the standard AAA RADIUS server.

If the same AAA group is configured with both the **aaa group** *aaa_group_name* and the **aaa secondary-group** *aaa_group_name* commands, then this configuration will have no effect and secondary accounting will not happen.

The AAA secondary server group configuration takes effect only when used with subscriber accounting-mode set to radius-diameter. The RADIUS accounting triggers for both standard RADIUS accounting and secondary accounting will be taken from the AAA group configured with the **aaa group** *aaa_group_name* command. On the fly change of this configuration is not supported. Any change to the configuration will have effect only for new calls.

Example

The following command applies the AAA server group *star1* to subscribers:

```
aaa group star1
```

access-link ip-fragmentation

Configures IP fragmentation processing over the Access-link.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

access-link ip-fragmentation { normal | df-ignore | df-fragment-and-icmp-notify }

df-ignore

Default: Enabled

Ignores the DF (Don't Fragment) bit setting. Fragments and forwards the packet over the access link.

df-fragment-and-icmp-notify

Default: Disabled

Partially ignores the DF bit. Fragments and forwards the packet, but also returns an ICMP error message to the source of the packet. The number of ICMP errors sent like this is rate-limited to one ICMP error packet per second per session.

normal

Default: Disabled

Normal processing. Drops the packet and sends an ICMP unreachable message to the source of packet. This is the default behavior.

Usage Guidelines

If the IP packet to be forwarded is larger than the access-link MTU and if the DF (Don't Fragment) bit is set for the packet, then the fragmentation behavior configured by this command is applied. Use this command to fragment packets even if they are larger than the access-link MTU.

Example

Set fragmentation so that the DF bit is ignored and the packet is forwarded anyway by entering the following command:

```
access-link ip-fragmentation df-ignore
```

accounting-mode

Sets the accounting mode for the current local subscriber configuration.

Product

PDSN

HA

ASN-GW

SAEGW

S-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

accounting-mode { flow-based | gtpp [radius-diameter] | none | radius-diameter [gtpp] | rf-style }
default accounting-mode

default

Sets the type of accounting to be performed for the current local subscriber to the default setting.

Default: **radius-diameter**

flow-based

Diameter flow-based accounting is enabled for the current local subscriber.

gtpp [radius-diameter]

GTPP CDR RADIUS accounting is enabled for the current local subscriber. The **radius-diameter** keyword is available if both GTPP RADIUS and RADIUS-Diameter accounting are to be used.

none

Accounting is disabled for the current local subscriber and no charging records will be generated.

radius-diameter [gtpp]

RADIUS-Diameter accounting is enabled for the current local subscriber. The **gtpp** keyword is available if both GTPP RADIUS and RADIUS-Diameter accounting are to be used.

rf-style

Diameter Rf interface accounting is enabled for the current local subscriber.

Usage Guidelines

This command specifies which protocol, if any, will be used to provide accounting for PDP contexts accessing the APN profile.

Use this command to enable or disable RADIUS/Diameter accounting for any subscribers that use the current local subscriber configuration.

If the **gtpp** option is used, then GTPP RADIUS is used as configured in the Context Configuration mode or the AAA Server Group Configuration mode and GTPP charging records will be enabled.

If the **radius-diameter** option is used, either the RADIUS or the Diameter protocol is used as configured in the Context Configuration mode or the AAA Server Group Configuration mode.

RADIUS accounting can also be enabled and disabled at the context level with the **aaa accounting** command in the Context Configuration Mode. If RADIUS accounting is enabled at the context level, the accounting-mode command can be used to disable RADIUS accounting for individual local subscriber configurations.

If the accounting mode is set to **rf-style**, then BM will generate accounting records corresponding to AIMS RF.

Example

To disable accounting for the current subscriber, enter the following command:

```
accounting-mode none
```

active-charging bandwidth-policy

Configures the bandwidth policy to be used for the subscriber.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

active-charging bandwidth-policy *bandwidth_policy_name*
{ default | no } active-charging bandwidth-policy

default

Specifies that the default bandwidth policy configured in the rulebase be used for this subscriber.

no

Disables bandwidth control for this subscriber.

active-charging bandwidth-policy *bandwidth_policy_name*

Specifies name of the bandwidth policy.

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

Usage Guidelines

Use this command to configure bandwidth policy to be used for subscribers.

Example

The following command configures a bandwidth policy named *standard* for the subscriber:

```
active-charging bandwidth-policy standard
```

active-charging link-monitor tcp

Enables the TCP link monitoring feature on the Mobile Video Gateway. This command can be configured in either APN Configuration Mode or Subscriber Configuration Mode.



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

Product

MVG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > **context** *context_name* > **subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

```
[ default | no ] active-charging link-monitor tcp [ log [ rtt [ histogram
 | time-series ] [ bitrate [ histogram | time-series ] ] | bitrate [
histogram | time-series ] [ rtt [ histogram | time-series ] ] ] ][
-noconfirm ]
```

default

Sets TCP link monitoring to its default value, which is the same as **[no]**.

no

Deletes the TCP link monitoring settings and disables TCP link monitoring if previously configured.

active-charging link-monitor tcp

Enables the TCP link monitoring feature on the Mobile Video Gateway. Note that TCP link monitoring is not enabled by default. Also note that when this command is configured without the **log** option, TCP link monitoring

is enabled without logging, and the output from TCP link monitoring is only used by the dynamic translating feature.

log [rtt [histogram | time-series] [bitrate [histogram | time-series]] | bitrate [histogram | time-series] [rtt [histogram | time-series]]]

This option enables statistical logging for TCP link monitoring.

The **rtt** option can be used to enable either **histogram** or **time-series** logging for round-trip time (RTT).

Similarly, the **bitrate** option can be used to enable either **histogram** or **time-series** logging for bit rate.

When **rtt** and **bitrate** options are used without additional options, histogram and time-series logging are enabled for round-trip time (RTT) and/or bit rate respectively.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to enable TCP link monitoring on the Mobile Video Gateway.

Examples

The following command enables TCP link monitoring with statistical logging, with histogram and time-series logging enabled for both RTT and bit rate:

```
active-charging link-monitor tcp log
```

The following command enables TCP link monitoring with statistical logging, with histogram and time-series logging enabled for RTT:

```
active-charging link-monitor tcp log rtt
```

The following command enables TCP link monitoring with statistical logging, with histogram logging enabled for RTT:

```
active-charging link-monitor tcp log rtt histogram
```

The following command enables TCP link monitoring with statistical logging, with histogram logging enabled for RTT and time-series logging enabled for bit rate:

```
active-charging link-monitor tcp log rtt histogram bitrate time-series
```

active-charging radio-congestion

Enables the Congestion Management feature on the Mobile Video Gateway. This command can be configured in either APN Configuration Mode or Subscriber Configuration Mode.



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

Product

MVG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-subscriber)#`

Syntax Description

active-charging radio-congestion policy *policy_name*

[default | no] active-charging radio-congestion policy

default

Sets congestion management to its default value, which is the same as **[no]**.

Default: Disabled

no

Deletes the settings and disables congestion management if previously configured.

active-charging radio-congestion policy *policy_name*

Enables the Congestion Management feature on the Mobile Video Gateway.

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

Usage Guidelines

Use this command to enable or disable congestion management on the Mobile Video Gateway at either APN or subscriber. As congestion management makes use of the Link Monitoring feature, this must also be enabled along with the congestion monitoring feature.

Example

The following command enables radio congestion for a policy named *test123* for the subscriber:

active-charging radio-congestion policy test123

active-charging rulebase

Specifies the rulebase to be used for this subscriber.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-subscriber)#`

Syntax Description

active-charging rulebase *rulebase_name*

no active-charging rulebase

no

Removes the previously configured rulebase for the subscriber.

active-charging rulebase *rulebase_name*

Specifies name of the ACS rulebase.

rulebase_name must be the name of an ACS rulebase expressed as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

This command specifies the name of the rulebase for specific subscriber (reals).

If the specified rulebase does not exist in the Active Charging service, the call will be rejected.

Example

The following command configures the ACS rulebase named *rule1* for the subscriber:

active-charging rulebase rule1

always-on

Once the idle timeout limit is reached, keeps the current subscriber session connected as long as the subscriber is reachable.



Caution When always-on is enabled, the subscriber must have an idle time-out period configured (default is 0, no time-out). Failure to configure an idle time-out results in a subscriber session that is indefinite.

Two timers and a counter are associated with this feature. Refer to the **timeout** command in this chapter and the **ppp echo-retransmit-timeout msec** and **ppp echo-max-retransmissions num_retries** commands.

Default: Disabled.

Product

PDSN

ASN-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax Description `[ no ] always-on`

always-on

Specifies that the user will remain connected after the idle time expires.

no

Disables **always-on**. The user is disconnected after the idle time expires.

Usage Guidelines If this parameter is enabled for a subscriber, when the idle time-out limit is reached the subscribers IP/PPP session remains connected as long as the subscriber is reachable. This is true even if the airlink between the mobile device and the RN (Radio Node) is moved from active to dormant (inactive) status. When the idle timeout limit is reached, the PDSN determines availability using link control protocol (LCP) keepalive messages. A response to these messages indicates that the "always-on" status should be maintained. Failure to respond to a predetermined number of LCP keepalive messages causes the PDSN to tear-down (disconnect) the subscriber session.

Example

Enable always on for the current subscriber by entering the following command:

```
always-on
```

asn-header-compression-rohc

Negotiates Robust Header Compression (ROHC) support for subscriber calls with AAA and WiMAX. This configuration indicates the type of header compression supported and enabled on the ASN.

Product ASN-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-subscriber)#`

Syntax Description `[ no | default ] asn-header-compression rohc`

no

Removes or disables the configured identifiers for ROHC in ASN-GW service.

default

The default is *disabled*.

Usage Guidelines Network Attached Storage (NAS) uses this configuration to indicate ROHC support of the subscriber TLV in the WiMAX-capability attribute within the Access Request. ROHC is applied only when ROHC is supported on the ASNGW and ROHC support is indicated by the AAA.

Example

The following command enables ROHC:

```
asn-header-compression rohc
```

asn nspid

Specifies the network service provider (NSP) associated with a WiMAX subscriber in an ASN-GW service. When configured, the NSP ID is sent in the Access-Request and Accounting messages.

Product ASN-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description **[no] asn nspid** *nsp_id*

no

Removes or disables the configured identifiers for this network service provider in ASN-GW service.

asn nspid *nsp_id*

Specifies the network service provider for this subscriber. This enables the MS to discover all accessible NSPs, and to indicate the NSP selection during connectivity to the ASN.

Usage Guidelines Use this command to specify the NSP associated with a subscriber in an ASN-GW service.

nsp_id is three bytes in hexadecimal format. For example: FF-EE-01

Example

The following command specifies the NSP for a subscriber in an ASN service:

```
asn nspid 0F-01-FE
```

asn-pdfid

Configures the identifiers for packet data flow, service data flow, and service profile in an ASN-GW service.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-subscriber)#`

Syntax Description

[no] asn-pdfid *pdf_id* **asn-service-profile-id** *svc_profile_id* **asn-sdfid** *sdf_id*

no

Removes/disables the configured identifiers for this subscriber in ASN-GW service.

asn-pdfid *pdf_id*

Specifies the an unique ASN Packet Data Flow identifier for this subscriber.

pdf_id must be an integer from 1 through 65535.

asn-service-profile-id *svc_profile_id*

Specifies a unique ASN Service Profile Identifier for this subscriber.

svc_profile_id is a Service Profile Identifier configured in the Context Configuration Mode.

asn-sdfid *sdf_id*

Specifies the an unique ASN Service Data Flow identifier for this subscriber.

sdf_id must be an integer from 1 through 65535.

Usage Guidelines

Use this command to configure subscriber profile for QoS parameters in an ASN-GW service.

A maximum of four QoS profiles can be configured for a subscriber.

Example

The following command configures the QoS profile for a subscriber as PDF id 1, Service Profile id 3, and Service Data Flow id 2:

```
asn-pdfid 1 asn-service-profile-id 3 asn-sdfid 2
```

asn-policy

Configures the identifiers for packet data flow, service data flow, and service profile in an ASN-GW service.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

```
asn-policy [classifiers downlink { strict | loose} | idle-mode { allow |
 disallow } | notification-idle-mode {allow | disallow} |
notification-handoff { allow | disallow }auth-only {allow | disallow } |
 ms-requested-classifiers {allow | dissalow}]
```

```
[ default ] asn-policy classifiers downlinkidle-mode
```

no

Removes or disables the configured policy for this subscriber in ASN-GW service.

default

Sets the ASN policy to default for this subscriber.

For downlink traffic classifier default policy is "loos" and for idle mode policy the default action is to allow idle mode operation in an ASN-GW service.

idle-mode

Sets the idle mode policy for this subscriber in an ASN-GW service. If enabled, Interim-Update is sent with the BSID and WiMAX-Idle_Mode Transition as Idle. If disabled, the Interim can be sent when the call is in the idle mode based on the interim timer. At this point, the last known BSID is reported to the RADIUS server.

notification-idle-mode

Default: allow

Use to enable or disable Idle-Mode-Notification capabilities. When you enable this command, when the call moves from active to idle, or idle to active, Accounting Interim is sent.

notification-handoff

Default: allow

If enabled, the Interim-Update is sent with the BSID and SN-Handoff-Indicator as Active Handoff.

allow

Default: enabled

Enables the policy for this subscriber to allow idle mode operation in an ASN-GW service.

disallow

Default: disabled

Enable the policy for this subscriber to disallow idle mode operation in an ASN-GW service.

classifiers downlink

Sets the classifier policy for all service flows coming from HA to FA for this subscriber's matching classifier.

strict

Default: disabled

This option discards all the service flows coming from HA to FA and any other packets not matching to any of the classifiers set for this subscriber.

loose

Default: enabled

This option allows all the service flows coming from HA to FA and any other packet does not matching to any of the classifiers set for this subscriber and sent to the BS/MS over downlink flow

auth-only

Specifies whether the call is Auth only or not.

allow

Enables the policy for this subscriber to allow auth-only in an ASN-GW service.

disallow

Default

Disables the policy for this subscriber to allow auth-only in an ASN-GW service.

ms-requested classifiers

Default: allow

By default ASNGW allows dynamic addition of classifiers by the MS during MS-initiated service flow creation or modification.

Usage Guidelines

Use this command to configure subscriber policy to allow/disallow the idle mode operation or the downlink traffic flow for a subscriber in an ASN-GW service.

For authentication configuration, the ASN-GW supports the Initial Network Entry (INE) for Ethernet CS calls. The base station supports Ethernet CS traffic to the network. The INE procedure includes the

Authentication of the service flows and IP-Address allocation through DHCP. Authentication is based on the Extensible Authentication Protocol (EAP).

This command allows MS to transition to idle mode with an ASN-GW.

Example

The following command configures the policy to allow the idle mode for an MS with an ASN-GW:

```
default asn-policy idle-mode
```

associate accounting-policy

Associates the subscriber with specific pre-configured policies configured in the same context.

Product

P-GW

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

[no] associate accounting-policy *name*

no

Removes the selected association from this subscriber.

name

Associates the subscriber with an accounting policy configured in the same context.

name must be an existing accounting policy expressed as a string of 1 through 63 characters.

Accounting policies are configured through the **policy accounting** command in the Context Configuration mode.

Usage Guidelines

Use this command to associate the subscriber with an accounting policy configured in this context.

Example

The following command associates this subscriber with an accounting policy called *acct1*:

```
associate accounting-policy acct1
```

authorized-flow-profile-id

When a profile ID is requested by the Mobile Node (MN), this command sets the value that is authorized by the Access Gateway (AGW).

Product

PDSN

ASN-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

authorized-flow-profile-id *profile_id* **direction { bidirectional | forward | reverse }**

no authorized-flow-profile-id *profile_id*

no

Removes the existing profile ID setting specified by *profile_id*. *profile_id* must be an integer from 0 through 65535.

authorized-flow-profile-id *profile_id*

The profile ID number that is authorized for the current subscriber. *profile_id* must be an integer from 0 through 65535.

direction { bidirectional | forward | reverse }

This specifies in which data direction the profile ID should be applied.

- **bidirectional**: This profile ID pertains to both the forward and reverse directions.
- **forward**: This profile ID pertains to data going to the MN.
- **reverse**: This profile ID pertains to data coming from the MN.

Usage Guidelines

Use this command to set the profile ID that the AGW will authorize for a subscriber.

Example

Set the profile ID for both directions to 3 for the current subscriber by entering the following command:

```
authorized-flow-profile-id 3 direction bidirectional
```

content-filtering category

Enables or disables the specified preconfigured Category Policy Identifier for policy-based Content Filtering support to the subscriber.

Product

CF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

content-filtering category policy-id *cf_policy_id*

no content-filtering category policy-id

no

Disables the configured category policy ID for content filtering support to the subscriber. This is the default setting.

content-filtering category policy-id *cf_policy_id*

Applies the content filtering category policy ID, configured in ACS Configuration Mode, to this subscriber.

cf_policy_id must be a category policy ID expressed as an integer from 1 through 4294967295.

If the specified category policy ID is not configured in the ACS Configuration Mode, all packets will be passed regardless of the categories determined for such packets.



Important Category Policy ID configured through this mode overrides the Category Policy ID configured using the **content-filtering category policy-id** command in the ACS Rulebase Configuration Mode.

Usage Guidelines

Use this command to enter the Content Filtering Policy Configuration Mode and enable or disable the Content Filtering Category Policy ID for a subscriber.



Important If Content Filtering Category Policy ID is not specified here, the similar command in the ACS Rulebase Configuration Mode determines the policy.

Up to 64 different policy identifier can be defined in a Content Filtering support service.

Example

The following command enters the Content filtering Policy Configuration Mode and enables the Category Policy ID *101* for Content Filtering support:

```
content-filtering category policy-id 101
```

credit-control-client

Configures the credit-control client parameters for the subscriber.

Product

GGSN

HA

IPSG

PDSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > **context** *context_name* > **subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

credit-control-client { event-based-charging | override session-mode { per-sub-session | per-subscriber } }

no credit-control-client { event-based-charging | override session-mode }

default credit-control-client event-based-charging

no

Disables the configured setting.

default

Resets the command to its default setting of disabled.

event-based-charging

Enables event-based charging.

override session-mode { per-sub-session | per-subscriber }

Overrides the session-mode configured through the CLI command "**require ecs credit-control session-mode per-subscriber**" in Global Configuration mode so that different subscriber groups can operate in different

modes. For example, one subscriber group can be configured to work in per-subscriber mode, while another in per-sub-session mode.

This keyword is used to switch between subscriber level Gy and sub-session level Gy.



Important This CLI can be changed on the fly. The modified values will be reflected only in the new subscriber session.

The **no** command removes the override CLI and makes the subscriber group fall back to the configuration specified through the CLI command "**require ecs credit-control session-mode per-subscriber**".

Usage Guidelines Use this command to configure the credit-control client parameters for the subscriber.

This configuration should be enabled to report UE's PLMN, timezone and ULI changes through Event-based-Gy session. In the event that both Gy Online charging and Gy event reporting are enabled, the P-GW shall send only CCR-Update requests to the OCS and shall not send CCR-Event requests.

With the inclusion of this keyword **override session-mode ...** in 14.1 release, it is possible to seamlessly change the configuration from bearer level to subscriber level and vice-versa without requiring a system reboot.

Example

The following command enables event-based Gy support for the subscriber:

```
credit-control-client event-based-charging
```

credit-control-group

Configures the credit-control group for this subscriber.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

```
credit-control-group cc_group_name
no credit-control-group
```

no

Removes the credit-control group from the subscriber configuration, if configured.

credit-control-group *cc_group_name*

Specifies name of the credit-control group.

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

Usage Guidelines

Use this command to configure the credit-control group for the subscriber.

Example

The following command configures the credit-control group named *test12* for the subscriber:

```
credit-control-group test12
```

credit-control-service

Configures the credit-control service for this subscriber.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

[no] credit-control-service *cc_service_name*

no

Disables the credit-control service, if configured.

credit-control-service *cc_service_name*

Specifies the name of the credit-control service.

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

Usage Guidelines

Use this command to configure the credit-control service for subscribers.

Example

The following command configures the credit-control service named *test12* for the subscriber:

```
credit-control-service test12
```

data-tunneling ignore df-bit

Controls the handling of the DF (Don't Fragment) bit present in the user IPv4/IPv6 packet for GRE, IP-in-IP tunneling used for the MIP data path. If this feature is enabled, and fragmentation is required for the tunneled user IPv4/IPv6 packet, then the DF bit is ignored and the packet is fragmented. Also the DF bit is not copied to the outer header. Default is enabled.

Product

PDSN

HA

FA

ASN-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

`[ no ] data-tunneling ignore df-bit`

no

Disables this option. The DF bit in the tunneled IP packet header is not ignored during tunneling.

data-tunneling ignore df-bit

Ignores the DF bit in the tunneled IP packet header.

Usage Guidelines

Use this command to configure a user so that during Mobile IP tunneling the DF bit is not ignored and packets are not fragmented.

Example

To disable fragmentation of a subscribers packets over a MIP tunnel even when the DF bit is present, enter the following command:

```
no data-tunneling ignore df-bit
```

dcca peer-select

Specifies the Diameter credit control primary and secondary peer for credit control.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

dcca peer-select peer *host_name* **[realm** *realm_name* **] [secondary-peer** *host_name* **[realm** *realm_name* **]]**

no dcca peer-select

no

Removes the previously configured Diameter credit control peer selection.

peer *host_name*

Specifies a unique name for the peer. *peer_name* must be an alphanumeric string of 1 through 63 characters that allows punctuation marks.

secondary-peer *host_name*

Specifies a back-up host that is used for fail-over processing. When the route-table does not find an available route, the secondary host performs a fail-over processing. *host_name* must be an alphanumeric string of 1 through 63 characters that allows punctuation marks.

realm *realm_name*

The *realm_name* must be an alphanumeric string of 1 through 63 characters that allows punctuation marks. The realm may typically be a company or service name.

Usage Guidelines

Use this command to select a Diameter credit control peer and realm.



Caution This configuration completely overrides all instances of **diameter peer-select** that have been configured with in the Credit Control Configuration Mode for an Active Charging service.

Example

The following command selects a Diameter credit control peer named *test* and a realm of *companyx*:

dcca peer-select peer test realm companyx

default

Restores the default value for the option specified for the current subscriber.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

```
default { access-link ip-fragmentation | accounting-mode | data-tunneling
 ignore df-bit | idle-timeout-activity dormant-downlink-data |
inter-pdsn-handoff | ip { alloc-method | allowed-dscp | header-compression
 | hide-service-address | multicast discard | qos-dscp | source-validation
 } | loadbalanace-tunnel-peers | long-duration-action | mobile-ip {
home-agent | mn-aaa-removal-indication | mn-ha-hash-algorithm |
reverse-tunnel | security-level | send { dns-address |
terminal-verification } } | permission | ppp { always-on-vse-packet |
data-compression { mode | protocols } | keepalive | min-compression-size
 | mtu } | radius accounting interim interval-timeout | timeout { absolute
 | idle } }
```

access-link ip-fragmentation

Sets the method for fragmenting packets over the MN access link to its default of normal. Drop the packet and send ICMP unreachable to the source of packet.

accounting-mode

Enables Radius accounting for the current local subscriber configuration.

data-tunneling ignore df-bit

Sets this option to the default behavior, which is to send an *ICMP unreachable - need to frag* message back to the sender and drop the packet, in the case that fragmentation is required but the DF bit is set.

idle-timeout-activity dormant-downlink-data

Sets this option to the default behavior. When downlink data packets are transmitted to the Mobile node and the session is in dormant mode the session idle timer is reset.

inter-pdsn-handoff

During a handoff from one PDSN to another, if the Mobile requests an IP address of 0.0.0.0 or a mismatched IP address the PDSN will not disconnect the session immediately. The PDSN tries to assign the proposed address of the session in the IPCP configuration NAK.

ip { alloc-method | allowed-dscp | dhcp-relay | header-compression | hide-service-address | multicast discard | qos-dscp | source-validation | user-datagram-tos copy }

allowed-dscp: resets the allowed DSCP parameters to the system defaults: class none, max-class be.

hide-service-address: specifies the default setting for hide the ip-address of the service from the subscriber. Default is Disabled

dhcp-relay: Configured with the DHCP server address during MS authentication. The AAA server sends the address of the DHCP server in the Access-Accept message. The DHCP relay uses this address to relay the DHCP messages from the MS to the DHCP server.

multicast discard: Configures the default multicast settings which is to discard PDUs

qos-dscp: Sets the quality of service setting to the system default.

source-validation: Specifies the default IP source validation. Default is Enabled.

user-datagram-tos copy: Disables copying of the IP TOS octet value to all tunnel encapsulation IP headers.

loadbalance-tunnel-peers

Sets the tunnel load balancing algorithm to the system default.

long-duration-action

Sets the action that is taken when the long duration timer expires to the default: detection.

mobile-ip { home-agent | mn-aaa-removal-indication | mn-ha-hash-algorithm | reverse-tunnel | security-level | send { dns-address | terminal-verification } }

allow-aaa-address-assignment: Disables the FA from accepting a home address assigned by an AAA server.

home-agent: Sets home agent IP address to its default of 0.0.0.0.

match-aaa-assigned-address: Disables the FA validating the home address in the RRQ against the one assigned by AAA server.

mn-aaa-removal-indication: Sets this parameter to its default of disabled.

mn-ha-hash-algorithm: Sets the encryption algorithm to the default of hmac-md5.

reverse-tunnel: Sets this parameter to its default of enabled.

security-level: Sets this parameter to its default of none.

send dns-address: Disables the HA from sending the DNS address NVSE in the RRP.

send terminal-verification: Disables the FA from sending the terminal verification NVSE in the RRQ.

permission

Restores the subscriber's service usage defaults.

ppp { always-on-vse-packet | data-compression { mode | protocols } | ip-header-compression negotiation | keepalive | min-compression-size | mtu }

Sets the point-to-point protocol option defaults.

always-on-vse-packet: Re-enables the PDSN to send special 3GPP2 VSE PPP packets to the Mobile Node with a max inactivity timer value for always on sessions. This configuration is applicable only for PDSN or PDSNCLOSED-RP sessions.

data-compression { **mode** | **protocols** }: restores the default value for either the data compression **mode** or compression **protocols** as follows:

- mode stateless
- all protocols enabled

ip-header-compression negotiation: Sets the IP header compressions negotiation to the system default: force.

keepalive: sets the subscriber's PPP keep alive option to the system default: 30 seconds.

min-compression-size: Restores the PPP minimum packet size for compression: 128 octets.

mtu: Sets the maximum message transfer unit packet size to the system default: 1500 octets.

radius accounting interim interval-timeout

Disables the RADIUS accounting interim interval for the current subscriber.

timeout [absolute | idle | long-duration]

When a keyword is entered, this command resets the specified timeout to the system default: 0. When no keyword is specified, all timeouts are reset to the system defaults: 0.

Usage Guidelines

Use this keyword to reset subscriber data to the system defaults. This is useful in setting the subscriber back to the basic values to possibly aid in trouble shooting or tuning a subscriber's access and options.

Example

The following CLI commands restore default values for various options:

```
default ip qos-dscp
default permission
default data-compression mode
```

description

Allows you to enter descriptive text for this configuration.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

```
description text
no description
```

no

Clears the description for this configuration.

text

Enter descriptive text as an alphanumeric string of 1 to 100 characters.

If you include spaces between words in the description, you must enclose the text within double quotation marks (" "), for example, "AAA BBBB".

Usage Guidelines

The description should provide useful information about this configuration.

Example

The following command enters the text description: *EO134 Anaheim*.

```
description "EO134 Anaheim"
```

dhcp dhcpv6

Specifies the DHCPv6 service to be used for this subscriber.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

dhcp dhcpv6 service-name *service_name*

no dhcp dhcpv6 service-name

no

Removes the DHCPv6 service for the subscriber.

dhcpv6 service-name *service_name*

Specifies the name of an existing DHCPv6 service to be used for this subscriber.

service_name must be the name of a DHCPv6 service expressed as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to apply or remove an existing DHCPv6 service to a subscriber template.

Example

The following command applies a previously configured DHCPv6 service named *dhcpv6_1* to a subscriber template:

```
dhcp dhcpv6 service-name dhcpv6_1
```

dhcp options

Specifies the DHCP options which can be sent from the DHCP server for this subscriber.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

dhcp options code 43 hex-values *hex_values*

no dhcp options

no

Removes the DHCP options for the subscriber.

options code 43 hex-values *hex_values*

Specifies hex values for DHCP option 43.

hex_values must be a dash-delimited list of hex data of size smaller than 506 datum.

Usage Guidelines

Use this command to specify the DHCP options which can be sent from the DHCP server for this subscriber.

Example

The following command applies hex values *ff-fe* for DHCP option 43:

dhcp options code 43 hex-values ff-fe

dhcp parameter-request-list-option

Enables the sending of DHCP parameter request list option(s) in all outgoing messages for this subscriber.

Product

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-subscriber)#`

Syntax Description

`[ no ] dhcp parameter-request-list-option [ options ]`

no

Disables the sending of DHCP parameter request list option(s) in all outgoing messages.

options

Specifies the value of particular DHCP parameter request list option(s).

options must be an integer from 1 through 254.



Important Multiple options may be selected in the same command.

Usage Guidelines

Use this command to enable or disable the sending of DHCP parameter request list option(s) in all outgoing messages for this subscriber.

Example

The following command enables DHCP parameter request list option inclusion in outgoing messages:

`dhcp parameter-request-list-option`

dhcp service



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

Enables DHCP service configuration accessible to the Se-GW context for subscriber. The specified DHCP service will be used for performing DHCP procedures between HNB-GW and HMS.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

dhcp service *dhcp_svc_name* **context** *ctxt_name*
no dhcp service

no

Removes the specified DHCP service from the subscriber template configuration.

dhcp_svc_name

Specifies name of the DHCP service configured in Context configuration mode for DHCP proxy support on HNB-GW.

dhcp_svc_name must be an alphanumeric string of 1 through 63 characters preconfigured within the same context of this subscriber.

context *ctxt_name*

Specifies the name of the context where DHCP service is configured for HNB-GW subscribers. *ctxt_name* must be an alphanumeric string of 1 trough 79 characters.

Usage Guidelines

This command associates the subscriber template with pre-configured DHCP service configuration to provide accessibility to Se-GW with HNB-GW.

Example

Following command applies a previously configured DHCP service named *dhcp_hnb1* to a subscriber template within the context named *femto_hnb*.

```
dhcp service dhcp_hnb1 context femto_hnb
```

dns

Configures the domain name servers for the current subscriber.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

[no] dns { primary | secondary } *ip_address*

no

Indicates the IP address is to be removed as either a primary or secondary domain name server.

dns primary | secondary

dns primary: Updates the primary domain name server for the subscriber.

dns secondary: Updates the secondary domain name server for the subscriber.

ip_address

Specifies the IP address of the domain name server using IPv4 dotted-decimal notation.

Usage Guidelines Set the subscriber DNS server lists as not all users will have the same set of servers.

Example

The following commands enable primary and secondary DNS servers for the subscriber:

```
dns primary 10.2.3.4
dns secondary 10.2.5.6
```

do show

Executes all **show** commands while in Configuration mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description

```
do show
```

Usage Guidelines Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



Caution There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

eap

Specifies the lifetime for a primary session key (PSK) for extensible authentication protocol (EAP) authentication.

Product ASN-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

In releases prior to StarOS 21.26:

[default] eap msk-lifetime *dur*

From StarOS 21.26 and later releases:

[default] eap psk-lifetime *dur*

psk-lifetime *dur*

Specifies the lifetime duration (in seconds) on Primary Session Key (PSK) in seconds for a WiMAX subscriber EAP authentication.

dur is an integer from 60 through 65535.

psk-lifetime *dur*

Specifies the lifetime duration (in seconds) on Primary Session Key (PSK) in seconds for a WiMAX subscriber EAP authentication.

dur is an integer from 60 through 65535.

Usage Guidelines

In releases prior to StarOS 21.26:

This command is used to set the lifetime for MSK in EAP authentication for WiMAX subscriber.

Example

The following command sets the lifetime for MSK key to *4800* seconds for a WiMAX subscriber through EAP authentication:

eap msk-lifetime 4800

From StarOS 21.26 and later releases:

Usage Guidelines

This command is used to set the lifetime for PSK in EAP authentication for WiMAX subscriber.

Example

The following command sets the lifetime for PSK key to *4800* seconds for a WiMAX subscriber through EAP authentication:

eap psk-lifetime 4800

encrypted password

Designates use of password encryption.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-subscriber)#`

Syntax Description **`encrypted password`** *`password`*

encrypted password *password*

password is the encrypted password and must be an alphanumeric string of 1 through 132 characters.

Usage Guidelines This command is normally used only inside configuration files.

Example

The following command sets an encrypted password of *qsdf12d4*:

`encrypted password qsdf12d4`

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.

external-inline-server

This is a restricted command.

firewall policy



Important This command is only available in StarOS 8.0. In StarOS 8.1 and later releases, this configuration is available in the ACS Rulebase Configuration Mode.

Enables or disables Stateful Firewall support for the subscriber.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-subscriber)#`

Syntax Description

`firewall policy firewall-required`

`{ default | no } firewall policy`

no

Disables Stateful Firewall support for this subscriber.

default

Configures the default setting for Stateful Firewall support.

Default: Disabled

firewall-required

Enables Stateful Firewall support for this subscriber.

Usage Guidelines Use this command to enable or disable Stateful Firewall support for this subscriber.

Important Unless Stateful Firewall support for this subscriber is enabled using this command, firewall processing for this subscriber is disabled.

Important If firewall is enabled, and the rulebase has no firewall configuration, Stateful Firewall will cause all packets to be discarded.

Example

The following command enables Stateful Firewall support for this subscriber:

```
firewall policy firewall-required
```

The following command disables Stateful Firewall support for this subscriber:

```
no firewall policy
```

fw-and-nat policy

Important This command is only available in StarOS 8.1. This customer-specific command must be used to configure the Policy-based Firewall-and-NAT feature.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

fw-and-nat policy *fw_nat_policy*

{ default | no } fw-and-nat policy

default

Specifies that the default Firewall-and-NAT policy configured in the rulebase be used for the subscriber.

no

Disables Firewall and NAT processing for the subscriber.

fw_nat_policy

Specifies the Firewall-and-NAT policy for the subscriber.

fw_nat_policy must be an alphanumeric string of 1 through 63 characters. Note that this policy will override the **default Firewall-and-NAT policy** configured in the ACS rulebase.

Usage Guidelines

Use this command to configure the Firewall-and-NAT policy for subscribers. Note that the policy configured in the subscriber mode will override the default policy configured in the ACS rulebase. If a policy is not configured in the subscriber mode, the default policy configured in the ACS rulebase will be applied.

Example

The following command configures a Firewall-and-NAT policy named *standard* for the subscriber:

```
fw-and-nat policy standard
```

gtpp

Configures GTP-P related parameters for a subscriber.

Product

IPSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

[default | no] gtpp { group | secondary-group } *group_name* **[accounting-context** *context_name* **]**

default

Resets the GTTP group name to the default group.

no

Deletes the specified group name.

group

Specifies primary group parameters.

secondary-group

Specifies secondary group parameters.

group_name

Specifies the name of the GTP-P group as an alphanumeric string of 1 through 63 characters.

accounting-context *context_name*

Specifies the GTPP accounting context as an alphanumeric string of 1 through 79 characters. Default is the GGSN service context.

Usage Guidelines

Use this command to enable or disable the generation of eG-CDRs for CDMA traffic observed in the customer network during IPSG deployment.

Example

The following command establishes the primary GTPP group *gtpp22*:

```
gtpp group gtpp22
```

idle-timeout-activity

Defines whether downlink (towards Mobile Node) data packets transmitted when the session is dormant are treated as activity for the idle-timer (inactivity timer).

By default, downlink data transmitted over a dormant session restarts the idle-timer for that session; it is treated as activity for the session.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

```
[ no ] idle-timeout-activity dormant-downlink-data
```

no

Dormant mode downlink data is not treated as activity for the session idle-timer. The session idle timer is not reset.

idle-timeout-activity dormant-downlink-data

Treats dormant mode downlink data as activity for the session idle-timer. The session idle timer is reset.

Usage Guidelines

Use this command to disable or re-enable restarting the session idle timer when downlink data packets are transmitted to the Mobile Node when the session is in dormant mode.

Example

Use the following command to disable restarting the session idle timer when downlink data packets are transmitted to the Mobile Node when the session is in dormant mode:

```
no idle-timeout-activity dormant-downlink-data
```

Use the following command to re-enable restarting the session idle timer when downlink data packets are transmitted to the Mobile Node when the session is in dormant mode:

```
idle-timeout-activity dormant-downlink-data
```

ikev2 tsr

Configures the Traffic Selector responder (TSr) negotiation behavior during IKEv2 Security Association (SA) establishment.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

```
[ default ] ikev2 tsr { wildcard | user-specified }
```

default

Specifies the default behavior, which is wildcard TSr negotiation.

ikev2 tsr

Enables TSr negotiation.

wildcard

Specifies that during TSr negotiation, the PDG/TTG always returns an any-to-any IP address range, an any-to-any port range, and allows any protocol, irrespective of the traffic selector ranges received from the UE. This is the default behavior.

user-specified

Specifies that during TSr negotiation, the PDG/TTG responds to each UE request with the UE-specified IP address ranges. This enables split tunneling on the PDG/TTG, and enables the UE to tunnel only a specified traffic range to the PDG/TTG and send other traffic directly out the WLAN.

Usage Guidelines

Use this command to specify the TSr negotiation behavior on the PDG/TTG.

Example

The following command enables user-specified TSr negotiation on the PDG/TTG:

```
ikev2 tsr user-specified
```

ims application-manager

Specifies the IP Multimedia Subsystem (IMS) application manager for the subscriber.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

[no] ims application-manager { domain-name *domain-name* **| ipv4-address** *ipv4_address* **}**

no

Disables the IMS application manager for this subscriber.

ims application-manager

Enables the IMS application manager for this subscriber.

domain-name *domain-name*

Specifies the domain name of the application manager.

domain-name must be an alphanumeric string of 1 through 63 characters.

ipv4-address *ipv4_address*

Specifies the IP address of the application manager using IPv4 dotted-decimal notation.

Usage Guidelines

The IMS application manager address is returned by HA to MN in DHCP Ack when it receives the DHCP inform from an AIMS subscriber.

Example

The following commands specify IMS application managers by domain name and IPv4 address:

```
ims application-manager domain-name domain23
ims application-manager ipv4-address 209.165.200.225
```

ims-auth-service

Enables IP Multimedia Subsystem (IMS) authorization support for subscriber. The specified IMSA service will be used for performing IMS authorization and flow-based charging procedures.

Product

PDSN

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

[default | no] ims-auth-service *auth_svc_name*

default

Configures default setting.

Default: Disabled or as specified at the context or network access service level or in subscriber template.

no

Removes the specified IMS authorization service from the subscriber configuration.

ims-auth-service *auth_svc_name*

Specifies name of the IMS authorization service.

auth_svc_name must be an alphanumeric string of 1 through 63 characters preconfigured within the same context of this subscriber.

Usage Guidelines

This feature provides the IMS authorization service configuration for Gx interface in IMS service node.

Example

The following command applies a previously configured IMS authorization service named *ims_interface1* to a subscriber within the specific context.

```
ims-auth-service ims_interface1
```

inter-pdsn-handoff

Configure the system to force the MN to use its assigned IP address during Internet Protocol Control Protocol (IPCP) negotiations resulting from inter-PDSN handoffs.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-subscriber)#`

Syntax Description

`[ no ] inter-pdsn-handoff require ip-address`

no

Disables the rejecting of sessions when the MN uses a non-allocated IP address during IPCP re-negotiations.

inter-pdsn-handoff require ip-address

Rejects sessions when the MN uses a non-allocated IP address during IPCP re-negotiations.

Usage Guidelines

This command is used to configure the system to reject sessions that are re-negotiating IPCP after an inter-PDSN handoff if the IP address they propose does not match the one initially provided by the PDSN. The session would be rejected even if the proposed address was 0.0.0.0.

If this parameter is disabled, the PDSN will attempt to re-assign the IP address initially provided.

Example

To set the PDSN to not allow a mismatched IP address during a PDSN to PDSN handoff of a MIP call, use the following command:

`inter-pdsn-handoff require ip-address`

To set the PDSN so that it will not disconnect the session immediately, if the Mobile requests an IP address of 0.0.0.0 or a mismatched IP address after inter-pdsn handoff, use the following command:

`no inter-pdsn-handoff require ip-address`

ip access-group

Configures IP access group for the current subscriber.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

`[ no ] ip access-group` *`group_name`* **`[ in | out ]`**

no

Indicates the access group specified is to be cleared from the subscribers configuration.

ip access-group *group_name*

Specifies the name of the IPv4/IPv6 access group. *acl_group_name* is a configured ACL group expressed as an alphanumeric string of 1 through 79 characters.

in | out

Default: both (in and out)

Specifies the access-group as either inbound or outbound by the keywords **in** and **out**, respectively. If neither of these key words is specified, the command associates the *group_name* access group with the current subscriber for both inbound and outbound access.

Usage Guidelines

Set the subscriber access group to manage the access control for subscribers as a logical group.

Example

The following command associates the *sampleGroup* access group with the current subscriber for both inbound and outbound access:

```
ip access-group sampleGroup
```

The following removes the outbound access group flag for *sampleGroup*:

```
no ip access-group sampleGroup out
```

ip address

Configures a static IPv4 address for use by the subscriber.

Product

PDSN

GGSN

HA

ASN-GW

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

`[ no ] ip address` *`ip_address netmask`*

no

Removes a previously configured IP address assignment.

ip address *ip_address*

Specifies the IP address assigned to the subscriber using IPv4 dotted-decimal notation.

netmask

The subnet mask that corresponds to the assigned IPv4 address.

Usage Guidelines

Use this command to assign a static IPv4 address to the subscriber. This address will be used each time the subscriber establishes data sessions.

Example

The following command configures a static IP address of *192.168.1.15* with a subnet mask of *255.255.255.224* to the subscriber:

```
ip address 192.168.1.15 255.255.255.224
```

ip address alloc-method

Configures the IP address allocation method for the current subscriber.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

```
ip address allocation-method { dhcp-client | dhcp-relay | local |
no-dynamic } [ allow-user-specified ]
```

dhcp-client

Default: Disabled

Configures the APN to assign an IP address received from a DHCP server.

Important If this option is used, the system's DHCP parameters must be configured.

dhcp-relay

Default: Disabled

Configures the APN to forward DHCP packets received from the MS to a DHCP server.

Important If this option is used, the system's DHCP parameters must be configured.

local

Default: Enabled

Configures the subscriber to dynamically receive IP addresses from a pool configured in the destination context on the system.

Important If this option is used, the name of the IP address pool from which to allocate addresses must be configured using the **ip address pool** command. If no pool name is specified, the system will attempt to allocate an address from any public pool configured in the destination context.

no-dynamic

Default: Disabled

Disables the dynamic assignment of IP addresses to sessions for this subscriber.

If a a session is received for this subscriber with this option enabled, it will be rejected with a cause code of 129, Registration Denied - administratively prohibited (for PDSN), 220, Unknown PDP address or PDP type (for GGSN).

allow-user-specified

Default: Enabled

Enables support for sessions requesting the use of specific (static) addresses.

Important If this option is not enabled, sessions requesting the use of a static address will be rejected with a cause code of 129, Registration Denied - administratively prohibited (for PDSN), 220 (Unknown PDP address or PDP type).

Usage Guidelines Use this parameter to dictate how dynamic IP addressing is to be handled for the subscriber when a static address is not provided.

Important When used in conjunction with the GGSN product, the settings for this command override those for the APN being accessed by the subscriber.

Example

The following command dictates that the subscriber is to receive a dynamically assigned address with the system configured as a DHCP client:

```
ip address alloc-method dhcp-client
```

ip address pool

Configures IP address pool properties for the subscriber.

Product

PDSN

GGSN

HA

ASN-GW

P-GW

SAEGW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

[no] ip address pool name *pool_name*

no

Removes a previously configured static address.

ip address pool name *pool_name*

Specifies the IP address pool or IP address pool group from which the subscribers IP address is assigned.

pool_name must be the name of an existing IP pool or IP pool group expressed as an alphanumeric string of 1 through 31 characters.

Usage Guidelines

Use this command to specify the name of an IP address pool configured on the system from which IP addresses are to be dynamically assigned to sessions from this subscriber.

This command can be issued multiple times to specify multiple address pools for the subscriber. If multiple pools are specified, addresses are assigned for subscriber sessions from the pools based on the order in which the pools were configured.

If an address cannot be provided from the first-specified pool for whatever reason, the system attempts to assign an address from the second-specified pool, and so on. This operation is independent of the priorities configured for the pools. For example, if pool1 was specified for the subscriber first, and pool2 second, the system always attempts to assign addresses from pool1. If an address can not be assigned from pool1 (i.e. all addresses are in use), the system then attempts to assign an address from pool2.

Example

The following command configures the subscriber to receive IP addresses from an IP address pool named *public1*:

```
ip address pool name public1
```

ip address secondary-pool

Configures secondary IP address pool properties for the subscriber to provide multiple IP host configuration behind one WiMAX Customer Premise Equipment (CPE).

Product

ASN-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

[no] ip address secondary-pool name *aux_pool_name*

no

Removes a previously configured auxiliary pool named *aux_pool_name* for multiple host support in ASN-GW service.

ip address secondary-pool name *aux_pool_name*

Specifies the secondary/auxiliary IP address pool or IP address pool group from which the IP address is assigned to host behind a WiMAX CPE having primary IP address.

pool_name must be the name of an existing IP pool or IP pool group expressed as an alphanumeric string of 1 through 31 characters.

Usage Guidelines

Use this command to specify the name of an IP address pool configured on the system from which IP addresses are to be dynamically assigned to host behind a WiMAX CPE for multiple host session support.

This command designates the IP address to secondary hosts from locally configured secondary IP address pool. To enable multiple host support behind a WiMAX CPE and configure maximum number of supported hosts use **secondary-ip-host** command in ASN Gateway Service Configuration mode.

Example

The following command configures the subscriber to receive IP addresses from a secondary IP address pool named *auxiliary1* for secondary hosts behind the WiMAX CPE:

```
ip address secondary-pool name auxiliary1
```

ip allowed-dscp

Sets the Quality of Service (QoS) Differentiated Services (DiffServ) marking that a subscriber session is allowed. The DSCP is disabled by default.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

ip allowed-dscp class *class* **max-class maxclass [rt-marking** *marking* **]**
no ip allowed-dscp class

no

Resets the parameters to the defaults: class none, max-class **be**. This indicates that all packets are let through without any dscp checking

ip allowed-dscp class *class*

Specifies the Differentiated Services Codepoint (DSCP) class with which the subscriber session may mark its packets. If the subscriber sessions packets request a code point class higher than the code point class specified, the PDSN service re-marks the packets with the QOS-DSCP value specified by the **ip qos-dscp** command.

Default: none

class must be one of the following;

a: allow packets with AF DSCPs

e: allow packets with EF DSCP

o: allow packets for experimental or local use

ae: allow packets with AF and EF DSCPs

ao: allow packets with AF DSCPs or packets for experimental or local use

eo: allow packets with EF DSCPs or packets for experimental or local use

aeo: allow packets with AF or EF DSCPs or packets for experimental or local use

none: allow only the **be** and **sc1** through **sc7** code points

max-class *maxclass*

This parameter specifies the maximum code point with which a subscriber session may mark its packets. The subscriber sessions packets must be marked with a code point equal to or less than the code point specified. If the subscriber sessions packets request a code point higher than the code point specified, the PDSN service re-marks the packets with the QOS-DSCP value specified by the lower of the max-class and the **ip qos-dscp** command.

The list below identifies the code points from lowest to highest precedence. For example, if the **maxclass** is set to af22, that becomes the maximum code point that the subscriber session may mark it's packets with and only **be, af13, af12, af11,af23**, and **af22** are allowed. If a subscriber session marks its packets with anything after af22 in this list, the PDSN service re-marks the packets with the QOS-DSCP value specified by the lower of the maxclass and the **ip qos-dscp** command.

If class is set to none only the be and sc1 through sc7 codepoints are allowed. For example; if **class** is set to none and you set **max-class** to **sc1**, only the **sc1** and **be** codepoints are allowed.

Default: **be**

maxclass must be one of the following;

be: best effort forwarding

af13: assured Forwarding 13

af12: assured Forwarding 12

af11: assured Forwarding 11

af23: assured Forwarding 23

af22: assured Forwarding 22

af21: assured Forwarding 21

af31: assured Forwarding 31

af32: assured Forwarding 32

af33: assured Forwarding 33

af41: assured Forwarding 41

af42: assured Forwarding 42

af43: assured Forwarding 43

ef: expedited forwarding

sc1: selector class 1

sc2: selector class 2

sc3: selector class 3

sc4: selector class 4

sc5: selector class 5

sc6: selector class 6

sc7: selector class 7

rt-marking *marking*

This parameter is used for Mobile IP (MIP) reverse tunnels. When MIP session packets do not have a DSCP marking, the Foreign Agent (FA) marks the packets with the value specified by **rt-marking** *marking*.

If MIP sessions packets have a DSCP marking, the marking is subjected to the conformance rules for the values of class and max-class; the final DSCP marking is then copied from the inner IP header to the outer IP header.

Default: **be**

marking must be one of the following;

be: best effort forwarding

af11: assured Forwarding 11

af12: assured Forwarding 12

af13: assured Forwarding 13

af21: assured Forwarding 21

af22: assured Forwarding 22

af23: assured Forwarding 23

af31: assured Forwarding 31

af32: assured Forwarding 32

af33: assured Forwarding 33

af41: assured Forwarding 41

af42: assured Forwarding 42

af43: assured Forwarding 43

ef: expedited forwarding

sc1: selector class 1

sc2: selector class 2

sc3: selector class 3

sc4: selector class 4

sc5: selector class 5

sc6: selector class 6

sc7: selector class 7

Usage Guidelines

Use this command to configure Quality of Service (QoS) for a subscriber session to allow a Differentiated Services (DiffServ) Code Point (DSCP) marker in the header of each IP packet that prompts network routers to apply differentiated grades of service to various packet streams.

This command uses **class** and type of marker (**rt-marking** for reverse tunnels) for configuration with **max-class** maximum code point that a subscriber session may mark its packets with.

Example

The following command will allow *o* packets for experimental or local use with best effort forwarding *be*:

```
ip allowed-dscp class o max-class be
```

ip context-name

Configures the context to which the subscriber is assigned upon authentication. The assigned context is considered the destination context that provides the configuration options for the services the subscriber is allowed to access.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

[no] ip context-name *name*

no

Removes the current assigned context from the subscriber's data.

ip context-name *name*

Specifies the name of the context to assign the subscriber to once authenticated. *name* must be an alphanumeric string of 1 trough 79 characters.

Usage Guidelines

Set the subscriber IP context to a common context when all subscribers from one or more contexts will use the same egress context.

Example

The following command specifies the IP context name *egress2*:

```
ip context-name egress2
```

ip header-compression

Configures the IP packet header compression options for the current subscriber. Although this command configures IP header compression algorithms, the Internet Protocol Control Protocol (IPCP) negotiations determine when the header compression algorithm is applied.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

ip header-compression { rohc [any [mode { optimistic | reliable | unidirectional }] | cid-mode { { large | small } [marked-flows-only | max-cid | max-hdr *value* **| mrru** *value* **] } | marked flows-only | max-hdr** *value* **| mrru** *value* **| downlink | uplink] | vj } +**

[default | no] ip header-compression

default

Restores this command's default setting to the Van Jacobsen (VJ) header compression algorithm.

no

Disables all IP header compression.

ip header-compression { rohc [any [mode { optimistic | reliable | unidirectional }] | cid-mode { { large | small } [marked-flows-only | max-cid | max-hdr *value* | mrru *value*] } } | marked flows-only | max-hdr *value* | mrru *value* | downlink | uplink] | vj }

Specifies that the Robust Header Compression (ROHC) algorithms is used for data.

Important ROHC is only supported for use with the PDSN.

any: Apply ROHC header compression in both the uplink and downlink directions.

mode { optimistic | reliable | unidirectional }:

- **optimistic**: Sets the ROHC mode to Bidirectional Optimistic mode (O-mode). In this mode packets are sent in both directions. A feedback channel is used to send error recovery requests and (optionally) acknowledgments of significant context updates from decompressor to compressor. Periodic refreshes are not used in the Bidirectional Optimistic mode.
- **reliable**: Sets the ROHC mode to Bidirectional Reliable mode (R-mode). This mode applies an intensive usage of a feedback channel and a strict logic at both the compressor and the decompressor that prevents loss of context synchronization between the compressor and the decompressor. Feedback is sent to acknowledge all context updates, including updates of the sequence number field.
- **unidirectional**: Sets the ROHC mode to Unidirectional mode (U-mode). With this mode packets are sent in one direction only, from the compressor to the decompressor. This mode therefore makes ROHC usable over links where a return path from the decompressor to the compressor is unavailable or undesirable.

cid-mode { { large | small } [marked-flows-only | dm | max-hdr *value* **| mrru** *value* **] }**: Specifies the ROHC packet type to be used.

- **large | small [marked-flows-only | max-cid | max-hdr** *value* **| mrru** *value* **]**: Defines the ROHC packet type as large or small and optionally sets the following parameters for the packet type selected:
- **marked-flows-only**: Specifies that ROHC is to be applied only to marked flows.
- **max-cid** *integer*: Default: 0 The highest context ID number to be used by the compressor. *integer* must be an integer from 0 through 15 when small packet size is selected and must be an integer from 0 through 31 when large packet size is selected.
- **max-hdr** *value*: Specifies the maximum header size to use. Default: 168. *value* must be an Integer from 0 through 65535.
- **mrru** *value*: Specifies the maximum reconstructed reception unit to use. Default: 65535. *value* must be an Integer from 0 through 65535.

marked-flows-only: Specifies that ROHC is to be applied only to marked flows.

max-hdr *value*: Specifies the maximum header size to use. Default: 168. *value* must be an Integer from 0 through 65535.

mrru *value*: Specifies the maximum reconstructed reception unit to use. Default: 65535. *value* must be an Integer from 0 through 65535.

downlink: Apply the ROHC algorithm only in the downlink direction.

uplink: Apply the ROHC algorithm only in the uplink direction.



Important When ROHC is enabled for downlink or uplink only the operational mode is Unidirectional.

vj

Specifies that the VJ algorithm is used for header compression.

+

Either one or both of the keywords may be entered in a single command.

If both **vj** and **rohc** are specified, **vj** must be specified first.

Important If both VJ and ROHC header compression are specified, the optimum header compression algorithm for the type of data being transferred is used for data in the downlink direction.

Usage Guidelines Header compression can be used to provide a higher level of security in IP traffic enhance bandwidth usage and lower bit errors.

By default the header compression algorithm is set to **vj**.

Example

The following command disables all IP packet header compression:

```
no ip header-compression
```

The following command sets IP header compression to default vj algorithm:

```
default ip header-compression
```

The following command also sets the IP header compression to the vj algorithm:

```
ip header-compression vj
```

The following command enables the Internet Protocol Control Protocol (IPCP) to determine which protocol is the optimum algorithm for data in the downlink direction and use either VJ or ROHC as needed:

```
ip header-compression vj rohc
```

The following command enables ROHC for the downlink direction only:

```
ip header-compression rohc downlink
```

The following command enables ROHC in any direction using Bidirectional Optimistic mode:

```
ip header-compression rohc any mode Optimistic
```

ip hide-service-address

Hides the IP address of the service from the subscriber.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

```
[ no ] ip hide-service-address
```

no

Does not hide the IP address of the service from the subscriber. This is the default behavior.

ip hide-service-address

Hides the IP address of the service from the subscriber.

Usage Guidelines

Use this command to prevent subscribers from using traceroute to discover the network addresses that are in the public domain and configured on services. This prevent users from pinging such addresses.

Example

The following command hides the IP address of the service from the subscriber:

```
ip hide-service-address
```

ip local-address

Configures the local-side IP address of the subscriber's point-to-point connection.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

```
ip local-address ip_address
no ip local-address
```

no

Removes a previously configured IP local-address.

ip_address *ip_address*

Specifies an IP address configured in a destination context on the system through which a packet data network can be accessed. *ip_address* is entered using IPv4 dotted-decimal notation.

Usage Guidelines

This parameter specifies the IPv4 address on the system that the MS uses as the remote-end of the PPP connection. If no local address is configured, the system uses an "unnumbered" scheme for local-side addresses.

Example

The following command configures a local address of 192.168.1.23 for the MS:

```
local-address 192.168.1.23
```

ip multicast discard

Configures the IP multicast discard packet behavior.

Product GGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description **`[ no ] ip multicast discard`**

no

Does not discard IP multicast packets.

ip multicast discard

Discards IP multicast packets.

Usage Guidelines This command specifies if IP multicast packets will be discarded.

Example

The following command discards IP multicast packets:

```
ip multicast discard
```

ip qos-dscp

Configures quality of service (QoS) options for the current subscriber using the differentiated services code point (DSCP) method. This functionality is disabled by default.

Product All

Privilege Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-subscriber)#`

Syntax Description

ip qos-dscp *option*
no ip qos-dscp

no

Sets the quality of service option to its default value.

ip qos-dscp *option*

Default: be (Best Effort)

Specifies the subscriber's per hop quality of service setting as one of:

- **af11**: assured Forwarding 11
- **af12**: assured Forwarding 12
- **af13**: assured Forwarding 13
- **af21**: assured Forwarding 21
- **af22**: assured Forwarding 22
- **af23**: assured Forwarding 23
- **af31**: assured Forwarding 31
- **af32**: assured Forwarding 32
- **af33**: assured Forwarding 33
- **af41**: assured Forwarding 41
- **af42**: assured Forwarding 42
- **af43**: assured Forwarding 43
- **be**: best effort forwarding
- **ef**: expedited forwarding

Usage Guidelines

Set the quality of service for a subscriber based upon the service level agreements.

Example

The following command specifies the QoS as expedited forwarding:

```
ip qos-dscp ef
```

ip route

Configures the static route to use to reach the subscriber's network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-subscriber)#`

Syntax Description

`[ no ] ip route` *`ip_address ip_mask`* **`[`** *`gateway_address`* **`]`**

no

Removes the configured route information from the subscriber data.

ip route *ip_address*

Specifies the target IP address for which the route information applies using IPv4 dotted-decimal notation.

ip_mask

Specifies the networking mask for the route.

1 bits in the *ip_mask* indicate that bit position in the *ip_address* must also have a value of 1.

0 bits in the *ip_mask* indicate that bit position in the *ip_address* does not need to match, such as the bit can be either a 0 or a 1.

For example, if the IP address and mask were specified as 172.168.10.0 and 255.255.255.224, respectively, the network mask will be 172.168.0.0 (obtained by logically ANDing the IP address with the IP mask).

gateway_address

Default: assigned remote IP address will be used as the gateway address.

Specifies the IP address of the next hop gateway for the route using IPv4 dotted-decimal notation.

Usage Guidelines

The static routes are also known as framed IP routes for subscribers. Static routes are typically applicable for subscribers connecting via other networks or when the mobile device acts as a gateway to a network on the far side of the device.

For example, if the mobile device is assigned IP address 10.2.3.4 and it acts as a gateway for the network 10.2.3.0 (with a network mask of 255.255.255.0) a static route would be configured with the *ip_address* being 10.2.3.0, *ip_mask* being 255.255.255.0, and *gateway_address* being 10.2.3.4.

Example

The following command disables the static route at IP address *10.2.3.4 255.255.255.0*.

```
no ip route 10.2.3.4 255.255.255.0
```

ip source-validation

Enables or disables packet source validation for the current subscriber. Source validation requires that the source address of the received packets match the IP address assigned to the subscriber (either statically or dynamically) during the session.

If an incorrect source address is received from the mobile node, the system attempts to renegotiate the PPP session. The parameters for IP source validation can be set by the **ip source-violation** command.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-subscriber)#`

Syntax Description

[no] ip source-validation

no

Disables source validation.

ip source-validation

Enables source validation.

Usage Guidelines

Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.

Example

The following command enables IP source validation:

```
ip source-validation
```

The following command disables IP source validation:

```
no ip source-validation
```

ip user-datagram-tos copy

Controls copying of the IP TOS octet value from IPv4/IPv6 datagrams to the IP header in tunnel encapsulation. This is disabled by default.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-subscriber)#`

Syntax Description

ip user-datagram-tos copy [access-link-tunnel | both | data-tunnel]

no ip user-datagram-tos copy

no

Disable copying of the IP TOS octet value to all tunnel encapsulation IP headers.

ip user-datagram-tos copy

Enables copying of the IP TOS octet value to all tunnel encapsulation IP headers.

access-link-tunnel

Copies the IP TOS octet value to the tunnel encapsulation IP header on the access side (RP) tunnel.

both

Uses both the access-link-tunnel and data-tunnel.

data-tunnel

Copies the IP TOS octet value to the tunnel encapsulation IP header on the MIP data tunnel or L3 tunnel (IP-in-IP, GRE).

Usage Guidelines

Use this command to enable the copying of the IP TOS octet value to the tunnel encapsulation IP header.

This functionality allows PCF to detect special TOS marking in the outer IP header of A11 packets and to identify certain packets as QChat control messages. The Base Station Controller/Packet Control Function (BSC/PCF) must give higher priority to QChat control messages.

Example

The following command enables copying of the IP TOS octet value to the tunnel encapsulation IP header for the access side tunnel:

ip user-datagram-tos copy access-link-tunnel

The following command disables copying of the IP TOS octet value to all tunnel encapsulation IP headers:

no ip user-datagram-tos copy

ip vlan

Configures subscriber-to-Virtual LAN (VLAN) associations.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

ip vlan *vlan-id*

[default | no] ip vlan

default

Resets the VLAN ID to the default setting.

no

Disables the VLAN ID for the subscriber.

ip vlan *vlan-id*

Specifies the VLAN ID that is associated with the IP address for that session. *vlan-id* is an integer from 1 through 4094.

Usage Guidelines

This command configures the subscriber vlan ID which is used with the assigned address for the subscriber session to receive packets. If the IP pool from which the address is assigned is configured with a VLAN ID, this subscriber configured VLAN ID overrides it.

Subscriber traffic can be routed to specific VLANs based on the configuration of their user profile. Using this functionality provides a mechanism for routing all traffic from a subscriber over the specified VLAN. All packets destined for the subscriber must also be sent using only IP addresses valid on the VLAN or they will be dropped.

Example

Set the vlan ID to the default setting by entering the following command:

```
default ip vlan
```

ipv6 access-group

Configures the IPv6 access group for a subscriber.

Product

PDSN

GGSN

ASN-GW

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-subscriber)#`

Syntax Description

`ipv6 access-group` *`name`* **`[ in | out ]`**

ipv6 access-group *name*

Defines the access group name. *name* is an alphanumeric string of 1 through 47 characters.

in

Defines the access group as inbound.

out

Defines the access group as outbound.

Usage Guidelines

Used to create an access group for a subscriber.

Example

The following command provides an example of an IPv6 access group with the name *list_1*:

`ipv6 access-group list_1`

ipv6 address

Configures a static IP address for use by the subscriber.

Product

PDSN

GGSN

ASN-GW

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-subscriber)#`

Syntax Description

`[ no ] ipv6 address { prefix` *`address`* **`| prefix-pool`** *`name`* **`}`**

no

Deletes a previously configured ipv6 address.

ipv6 address *address*

Specifies an IPv6 address. *address* is entered using IPv6 colon-separated-hexadecimal notation.

prefix

Specifies a static IPv6 address.

prefix-pool *name*

Specifies an IPv6 prefix pool name. *name* is an alphanumeric string of 1 through 31 characters.

Usage Guidelines

Use this command to assign a static IPv6 address to the subscriber. This address will be used each time the subscriber establishes data sessions.

Example

The following command configures a static IP address of *2001:4A2B::1f3F* with a mask length of *24* to the subscriber:

```
ipv6 address 2001:4A2B::1f3F/24
```

ipv6 dns

Configures the IPv6 Domain Name Service (DNS) servers.

Product

PDSN

GGSN

ASN-GW

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-subscriber)#`

Syntax Description

`[ no ] ipv6 dns { primary | secondary } {` *`ipv6_dns_address`* **`}`**

no

Deletes a previously configured DNS server.

ipv6 dns *ipv6_dns_address*

Specifies an IP address for the DNS server. *ipv6_dns_address* is entered using IPv6 colon-separated-hexadecimal notation.

primary

Configures the primary DNS server for the subscriber.

secondary

Configures the secondary DNS server for the subscriber. Only one secondary DNS server can be configured.

ipv6_dns_address

Configures the IP address of the DNS server.

Usage Guidelines

DNS servers are configured on a per subscriber basis. This allows each subscriber to use specific servers.

Example

The following command provides an example of setting the primary IPv6 DNS server:

`ipv6 dns primary fe80::c0a8:a04`

ipv6 dns-proxy

Configures the system to act as a domain name server proxy for the current subscriber.

Product

PDSN

GGSN

ASN-GW

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-subscriber)#`

Syntax Description

[default | no] ipv6 dns-proxy

default

Disables IPv6 DNS proxy functionality for a subscriber.

no

Removes the pre-enabled functionality of IPv6 DNS proxy for a subscriber.

ipv6 dns-proxy

Enables IPv6 DNS proxy functionality for a subscriber. If enabled, the system will act as a proxy DNS server.

Default: disabled.

Usage Guidelines

Used to enable or disable IPv6 DNS proxy for the subscriber. When enabled, the PDSN acts as a proxy DNS server for DNS IPv6 queries coming from the mobile station to the PDSN's local PPP link address.

Example

The following command disables the IPv6 DNS proxy function for the subscriber:

no ipv6 dns-proxy

ipv6 egress-address-filtering

Configures the system to perform egress address filtering for the subscriber.

Product

PDSN

GGSN

ASN-GW

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > **context** *context_name* > **subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

```
[ no ] ipv6 egress-address-filtering
```

no

Disables IPv6 egress address filtering.

ipv6 egress-address-filtering

Enables IPv6 egress address filtering.

Usage Guidelines

Used to enable the filtering of packets that arrive from the Internet to a particular site.

Example

The following command disables egress address filtering:

```
no ipv6 egress-address-filtering
```

ipv6 initial-router-advt

Creates an IPv6 initial router advertisement interval for the subscriber.

Product

PDSN

GGSN

ASN-GW

HSGW

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > **context** *context_name* > **subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

```
ipv6 initial-router-advt { interval value | num-advts value |
router-solicit-wait-timeout value }
default ipv6 initial-router-advt { interval | num-advts |
router-solicit-wait-timeout }
no ipv6 initial-router-advt router-solicit-wait-timeout
```

default

Resets the command to its default settings.

no ipv6 initial-router-advt router-solicit-wait-timeout

Disables running timer to wait for router solicit and sends the initial router advertisement immediately once session is up.

ipv6 initial-router-advt

Enables an initial router advertisement interval in milliseconds.

interval *value*

Default: 3000

The time interval the initial IPv6 router advertisement is sent to the mobile node in milliseconds.

value is an integer between 100 and 16000 milliseconds.

num-advts value *value*

Default: 3

The number of initial IPv6 router advertisements sent to the mobile node. *value* is an integer between 1 to 16.

router-solicit-wait-timeout *value*

Default: 3000

The time interval to wait for router solicit before sending the initial IPv6 router advertisement.

value is an integer between 1 and 30000 milliseconds.

Usage Guidelines

This command is used to set the advertisement interval and the number of advertisements. Using a smaller advertisement interval increases the likelihood of router being discovered more quickly when it first becomes available.

If timer is enabled and router solicit is received before timeout, then RA will be sent in response to RS and no further RA will be sent. If timer is enabled and no router solicit is received after timeout, initial RAs will be sent as configured and IPv6 capability indication will be sent in S2a to P-GW to indicate that P-GW should drop any IPv6 traffic for this PDN.

Example

The following command specifies the initial ipv6 router interval to be 2000ms:

```
ipv6 initial-router-advt interval 2000
```

ipv6 interface-id

Provides an IPv6 interface identifier for the subscriber.

Product

PDSN

GGSN

ASN-GW

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

ipv6 interface-id *ifid*

[default | no] ipv6 interface-id

default

No interface ID set for IPv6CP negotiation to subscriber.

no

Deletes a previously configured IPv6 interface ID.

interface-id *ifid*

Specifies the interface ID assigned to the Mobile during IPv6 Control Protocol (IPv6CP) negotiation. *ifid* is a 64-bit unsigned integer.

Usage Guidelines

Used to provide a IPv6 ifid for the subscriber when using IPv6-to-IPv4 (6to4) routing.

Example

The following command provides an example of assigning an IPv6 interface ID of *00-00-00-05-47-00-37-44* to the subscriber:

```
ipv6 interface-id 00-00-00-05-47-00-37-44
```

ipv6 minimum-link-mtu

Configures the IPv6 minimum link maximum transmission unit (MTU) value.

Product

PDSN

GGSN

ASN-GW

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

ipv6 minimum-link-mtu *value*

default ipv6 minimum-link-mtu

default

Resets minimum link MTU to its default setting: 1280.

ipv6 minimum-link-mtu *value*

Specifies the MTU (in bytes) as a minimum link value. *value* is an integer between 100 and 2000.

Usage Guidelines

Used to override the IPv6 minimum link MTU values recommended by the standard.

Example

The following command provides an example of assigning an IPv6 minimum link MTU to *1580* to the subscriber:

```
ipv6 minimum-link-mtu 1580
```

ipv6 secondary-address

Configures additional IPv6 4-bit prefixes to the subscriber session.

Product

PDSN

GGSN

ASN-GW

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

[no] ipv6 secondary-address { prefix *ipv6_address_prefix* **| prefix-pool** *pool_name* **}**

no

Deletes a previously configured ipv6 secondary address.

ipv6 secondary-address *ipv6_address_pref*

Specified the secondary IPv6 address using IPv6 colon-separated-hexadecimal notation.

pool_name

Specifies the name given to the secondary address prefix pool as an alphanumeric string of of 1 through 31 characters.

Usage Guidelines

An IPv6 prefix pool name may be configured for a dynamic prefix, while the prefix is static. This command may be executed multiple times to configure multiple prefixes.

Example

The following command assigns an IPv6 secondary address prefix-pool name of *eastcoast* to the subscriber:

```
ipv6 secondary-address prefix-pool eastcoast
```

l2tp send accounting-correlation-info

Enables the sending of accounting correlation information (Correlation-Id, NAS-IP-Address and NAS-ID) by the L 2TP Access Concentrator (LAC) in L2TP control messages (ICRQ) during session setup to an L2TP Network Server (LNS).

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

[no | default] l2tp send accounting-correlation-info

no

Disables the sending of accounting correlation information by the LAC.

default

Sets the setting to default mode: disable.

l2tp send accounting-correlation-info

Enables the sending of accounting correlation information by the LAC.

Usage Guidelines

Use this command to enable the LAC to send accounting correlation information (Correlation-Id, NAS-IP-Address and NAS-ID) in L2TP control message (ICRQ) during session setup to LNS for this subscriber. LNS can be configured to include this information in ACS billing records, so that billing servers can easily correlate accounting records from PDSN/LAC and LNS.

By default, this mode is disabled.

Example

The following command disables the inclusion of accounting correlation information in control messages during session setup to an LNS for a subscriber:

```
default l2tp send accounting-correlation-info
```

l3-to-l2-tunnel address-policy

Configures the subscriber address allocation/validation policy, when subscriber Layer 3 (IPv4) sessions are tunneled using Layer 2 tunneling protocol (L2TP).

Product

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

l3-to-l2-tunnel address-policy { alloc-only | alloc-validate | no-alloc-validate }

default l3-to-l2-tunnel address-policy

default

Restores the default value for Layer 3-to-Layer 2 tunnel addressing: **no-alloc-validate**.

l3-to-l2-tunnel address-policy

Sets the policy for Layer 3-to-Layer 2 sessions to one of the following options.

alloc-only

Only allocates an address in the case of dynamic address assignment. Does not validate static addresses.

alloc-validate

Locally allocates and validates the subscriber addresses.

no-alloc-validate

Does not allocate or validate subscriber addresses locally for current subscribers sessions. Passes the address between the remote tunnel terminator and the Mobile Node. This is the default behavior.

Usage Guidelines

Use this command to configure the L3 to L2 tunnel address policy for MIP HA sessions tunneled from the system using L2TP tunnels or for GGSN IP Context sessions tunneled using L2TP to a remote LNS. Also refer to the **resource** keyword of the Context Configuration mode **ip pool** command.

Example

the following command sets the L3-to-L2 tunnel address policy so that the current subscriber must have IP addresses allocated and validated locally on the system:

```
l3-to-l2-tunnel address-policy alloc-validate
```

loadbalance-tunnel-peers

Configures the load balancing of traffic bound for L2TP tunnels configured on the system for the selected subscriber.

Product

L2TP

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

```
loadbalance-tunnel-peers { balanced | prioritized | random }
```

loadbalance-tunnel-peers

Enables load balancing of L2TP traffic using one of the methods described below.

balanced

Enables the equal use of all configured tunnel peers (LNSs) for the selected subscriber.

prioritized

Enables the use of all configured tunnel peers (LNSs) for the selected subscriber based on the preference number assigned to the peer address.

random

Default: Enabled

Enables the random use of all configured tunnel peers (LNSs) for the selected subscriber.

Usage Guidelines

Use to manage traffic loads on L2TP Access Concentrator (LAC) ports and their respective L2TP Network Servers (LNSs).

Example

Use the following command to randomly use all configured tunnel peers (LNSs):

```
loadbalance-tunnel peers random
```

long-duration-action

Specifies what action is taken when the long duration timer expires.

Product

All

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

```
long-duration-action { detection | disconnection [ dormant-only ] [
suppress-notification ] }
```

detection

Default: Enabled

Detects long duration sessions and sends SNMP TRAP and CORBA notification. This is the default behavior.

Use this command to detect a session exceeding the limit set by the long duration timer.

disconnection [dormant-only] [suppress-notification]

Default: Disabled

Detects a long duration session and disconnects the session after sending SNMP trap and CORBA notification.

suppress-notifiaction: Suppresses the SNMP trap and CORBA notification after detecting and disconnecting a long duration session. Default: Disabled

dormant only: Disconnects the dormant sessions after long duration timer and inactivity time with idle time-out duration expires. If the long duration timeout is fired and the call is not dormant, the call is disconnected when the call later moves to dormancy.



Important For HA calls, the inactivity-time is considered as gauge for dormancy.

It sends the SNMP trap and CORBA notification after disconnecting a long duration session. Default: Disabled

Usage Guidelines Use this command to determine what action is taken when a session exceeds the limit set by the long duration timer.

Example

Use the following command to enable disconnecting sessions that exceed the long duration timer:

```
long-duration-action disconnection
```

Use the following command to disconnect the session that exceed the long duration timer without sending SNMP trap and CORBA notification:

```
long-duration-action disconnection suppress-notification
```

Use the following command to disconnect the session that is in dormant and exceed the long duration timer and send SNMP trap and CORBA notification:

```
long-duration-action disconnection dormant-only
```

Note that in case of HA calls, the inactivity-time is considered as gauge for dormancy.

max-pdn-connections

Specifies the maximum number of connections to packet data networks (PDNs) supported per eHRPD session.

Product HSGW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

```
max-pdn-connections eHRPD_PDNs
default max-pdn-connections
```

default

Resets the maximum number of PDN connections supported per eHRPD session to 3.

max-pdn-connections *eHRPD_PDNs*

Specifies the maximum number of PDN conceitedness allowed per eHRPD session. *eHRPD_PDNs* must be an integer from 1 to 14. Default is 3.

Usage Guidelines

This command is used to specify the maximum number of PDN connections supported per eHRPD session.

Example

The following command specifies a maximum of 5 PDNs per eHRPD session:

```
max-pdn-connections 5
```

mediation-device

Enables the use of a mediation device for subscribers, and specifies the system context to use for communicating with the device. A mediation device can be the initial point of contact for all IT systems that need to receive Charging Data Records (CDRs). Mediation devices can also be deep-packet inspection servers or transaction control servers.

Product

GGSN

P-GW

PDG/TTG

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

`mediation-device context-name` *<context-name>* **`[ no interims ]`**

`[ no | default ] mediation-device`

no

Deletes the mediation-device configuration.

default

Changes the mediation device to no context-name configured and restores the mediation device's default properties.

mediation-device context-name *context-name*

Default: The subscriber's destination context.

Configures the mediation VPN context for the subscriber.

context-name must be an alphanumeric string of 1 through 79 characters that is case sensitive. If not specified, the mediation context is same as the destination context of the subscriber.

no-interims

Disables sending of Interim messages to the mediation device.

Default: Disabled

Usage Guidelines

This command is used to enable mediation device support for subscribers.

Keywords to this command can be used in combination to each other, depending on configuration requirements.

Example

The following command enables mediation device support for the subscriber and uses the protocol configuration located in an system context called *ggsn1*:

```
mediation-device context-name ggsn1
```

mobile-ip

Enables or disables access to mobile IP services by the subscriber.

Product

HA

FA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

```
[ no ] mobile-ip { allow-aaa-address-assignment | dns-address
source-priority { aaa | home-agent } | gratuitous-arp aggressive |
home-agent ip_address [alternate] | match-aaa-assigned-address |
min-reg-lifetime-override [value | infinit ] | mn-aaa-removal-indication
| mn-ha-hash-algorithm { hmac-md5 | md5 | rfc2002-md5 } | mn-ha-shared-key
 key | mn-ha-spi spi_num | reverse-tunnel | security-level { ipsec | none
} | send {access-technology | accounting-correlation-info bsid |
dns-address | host-config | imsi | terminal-verification } }
```

no

Disables the mobile IP option specified.

allow-aaa-address-assignment

Default: Disabled.

Enables the FA to accept a home address assigned by an AAA server. This should only be configured on the FA side.

dns-address source-priority { aaa | home-agent }

Sets the priority behavior on the FA to use either the DNS IP address information from the HA or the AAA server to include in the RRP to the MN.

When the **no** keyword is used in conjunction with the **dns-address** keyword, information received from both the home-agent and the AAA server is sent if available.

DNS IP address information from the HA comes from the DNS Normal Vendor/Organization Specific Extension (NVSE) in the Registry Registrar Protocol (RRP).

DNS IP address information from the AAA server is in the access accept message.

home-agent: If the DNS address is received from the home-agent only that information is sent to the MN. Otherwise the DNS address received from the AAA server is sent.

aaa: If the DNS address is received from the AAA server only that information is sent to MN. Otherwise the DNS address received from the home-agent is sent.

gratuitous-arp aggressive

Default: Disabled.

When enabled, this mode will cause the HA to send out gratuitous ARP (Address Resolution Protocol) messages for all Mobile IP (MIP) registration renewals and handoffs.

To disable this mode, use the **no** form of this command.



Important This mode will only work for IP addresses that have been assigned from a static IP address pool.

home-agent *ip_address* [alternate]

Specifies the IP address of the mobile IP user's home agent. *ip_address* must be entered using IPv4 dotted-decimal or IPv6 colon -separated notation.

alternate - Specifies the secondary, or alternate, Home Agent to use when Proxy Mobile IP HA Failover is enabled.

match-aaa-assigned-address

Default: Disabled.

Enables the FA to validate the home address in the RRQ against the one assigned by AAA server. This should only be configured on the FA side.

min-reg-lifetime-override [*value* | infinit]

Default: 0.

Configures the subscriber for minimum registration lifetime parameter on HA service. By default it uses the value configured on HA service where *value* must be the minimum registration lifetime that the HA service allows in any Registration Request message from the mobile node. An infinite registration lifetime can be configured by setting the value as "infinite".

value is a minimum registration lifetime value in seconds and must be an integer between 1 through 65534.

mn-aaa-removal-indication

Default: Disabled.

When enabled, the MN-FA challenge and MN-AAA Authentication extensions are removed when relaying a Registration Request (RRQ) to the Home Agent (HA)

mn-ha-hash-algorithm { hmac-md5 | md5 | rfc2002-md5 }

Speechifies the encryption algorithm to use.

Default: **hmac-md5**

hmac-md5: Uses HMAC-MD5 hash algorithm, as defined in RFC-2002bis. This is the default algorithm.

md5: Uses the MD-5 hash algorithm.

rfc2002-md5: Uses the MD-5 hash algorithm variant as defined in RFC-2002.

mn-ha-shared-key *key*

Verifies the MN-HA Authentication for a local subscriber in the current context. *key* is an alphanumeric string or a hexadecimal number beginning with "0x" up to 127 bytes

mn-ha-spi *spi_num*

Specifies the Security Parameter Index (SPI) number. *spi_num* must be an integer from 256 through 4294967295.

reverse-tunnel

Default: enabled.

All the mobile IP user to use reverse IP tunnels. The **no** keyword disables this option.

security-level { ipsec | none }

Default: none

Configures the security level needed for the subscriber's traffic.

ipsec: secures both MIP control and data traffic with IPSec.

none: none of the traffic is secured



Important This keyword corresponds to the 3GPP2-Security-Level RADIUS attribute. This attribute indicates the type of security that the home network mandates on the visited network.

Important For this attribute, the integer value "3" enables IPSec for tunnels and registration messages, "4" Disables IPSec

send {access-technology | accounting-correlation-info bsid | dns-address | host-config | imsi | terminal-verification }

access-technology: Configures FA to sends the access-technology type extension in the RRQ, by default it is disabled.

accounting-correlation-info: Configures whether the FA sends the correlation info to the NVSE in the RRQ. Default is disabled.

dns-address: Enables the HA to send the DNS address NVSE in the RRP. Default is disabled. This should only be enabled on the HA side.

host-config: Configures by sending the Host Config NVSE in RRQ. By default it is disabled.

imsi: Configures sending the IMSI NVSE in the RRQ. Default is sending IMSI in custom-1 format.

terminal-verification: Enables the FA to send the terminal verification NVSE in the RRQ. Default is disabled. This should only be enabled on the FA side.

Important **send dns-address** is a proprietary feature developed for a specific purpose and requires the MN to be able to renegotiate IPCP for DNS addresses and reregister MIP if necessary. Since this feature needs the MN to support certain PPP/MIP behavior, and not all MNs support that particular behavior, **send dns-address** should be enabled only after careful consideration.

Usage Guidelines Use as subscriber service contracts change.

Example

The following command specifies the Home Agent at *10.2.3.4* for this subscriber:

```
mobile-ip home-agent 10.2.3.4
```

mobile-ip ha

Accommodates two Mobile IP (MIP) Home Agent (HA) options in subscriber mode.

Product PDSN

HA

ASN-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

[no] mobile-ip ha { assignment-table *name* **| ignore-unknown-ha-addr-error }**

no

Disables the mobile IP HA option specified.

assignment-table *name*

Specifies the name of an existing MIP HA Assignment table. *name* must be an alphanumeric string of 1 through 63 characters.

ignore-unknown-ha-addr-error

Default is disabled.

Enables or disables the HA to accept or reject the RRQ from a particular subscriber.

Usage Guidelines

Use this command to assign a MIP HA Assignment table to the current subscriber.

Use this command to disable or enable the HA to accept or reject the RRQ from a particular subscriber when the HA address in the incoming MIP RRQ is not the same as the HA service address. The feature is off by default which causes the RRQ to be rejected with the error code UNKNOWN_HOME_AGENT.

Example

The following command assigns the MIP HA Assignment table named *Atable1* to the current subscriber:

```
mobile-ip ha assignment-table Atable1
```

The following command sets **ignore-unknown-ha-addr-error** to its default disabled state:

```
no mobile-ip ha ignore-unknown-ha-addr-error
```

mobile-ip reg-lifetime-override

Overrides the Mobile IP (MIP) registration lifetime from HA with value configured for subscriber.

Product

PDSN

HA

ASN-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

mobile-ip reg-lifetime-override [*dur* | infinite]

[default | no] mobile-ip reg-lifetime-override

mobile-ip reg-lifetime-override*dur*

Default: 100 seconds.

Overrides the MIP registration lifetime from HA for the specified period of time in seconds. *dur* must be an integer from 1 through 65534.

infinite

Sets the MIP registration lifetime override value to infinite for a particular subscriber.

default

Sets the value of mobile IP registration lifetime override option to 100 seconds.

no

Disables the MIP registration lifetime override option.

Usage Guidelines

Use this command to configure MIP registration-lifetime per realm/domain. This value overrides the default lifetime configured under HA service.

Example

The following command overrides the MIP registration lifetime value from HA service and defaults the MIP registration lifetime to 100 seconds for the current subscriber:

default mobile-ip reg-lifetime-override

mobile-ip send access-technology

Enables the sending of the RAT (Radio Access Technology) of the MS to the HA in a PMIP RRQ (Proxy MIP Register Request) message.

Product

PDIF

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

[default | no] mobile-ip send access-technology

default

Disables the support for sending the RAT to the HA in a PMIP RRQ.

This is the default mode.

no

Removes the configured support for sending the RAT to the HA in a PMIP RRQ.

Usage Guidelines

Use this command to send the RAT to the HA in a PMIP RRQ.

Example

The following command enables sending the RAT to the HA in a PMIP RRQ:

mobile-ip send access-technology

mobile-ip send accounting-correlation-info

Enables the sending call correlation information Normal Vendor/Organization Specific Extensions (NVSEs) to the HA in the MIP Registry Registrar Protocol (RRP).

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

[default | no] mobile-ip send accounting-correlation-info

default

Disables the support for sending call correlation information NVSEs to the HA in MIP RRQ.

This is the default mode.

no

Removes the configured support for sending call correlation information.

Usage Guidelines

Use this command to support PDSN-Correlation-ID VSE and send the call correlation information.

Example

The following command enables sending call correlation information NVSEs to the HA in MIP RRQ:

```
mobile-ip send accounting-correlation-info
```

mobile-ip send bsid

Enables the sending of the BSID (Base Station Identifier) of the WiFi access point/Radio Access Network (RAN) to the HA in a PMIP RRQ (Register Request) message.

Product

PDIF

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

mobile-ip send bsid [custom-2]

[default | no] mobile-ip send bsid

default

Disables the support for sending the BSID to the HA in a PMIP RRQ.

This is the default mode.

no

Removes the configured support for sending the BSID to the HA in a PMIP RRQ.

custom-2

NVSE to send service option attribute in the PMIP RRQ.



Important This is a customer-specific keyword and needs customer-specific license to use this feature.

Usage Guidelines

Use this command to send the BSID to the HA in a PMIP RRQ.

Example

The following command enables sending the BSID to the HA in a PMIP RRQ:

```
mobile-ip send bsid
```

mobile-ip send pcf-address

Configures whether the FA sends the PCF address NVSE in the RRQ.

Product



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

HA

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

mobile-ip send pcf-address [custom-2]

[default | no] mobile-ip send pcf-address

default

Disables the support for sending the PCF address to the HA in a PMIP RRQ.

This is the default mode.

no

Removes the configured support for sending the PCF address to the HA in a PMIP RRQ.

custom-2

NVSE to send PCF address attribute in the PMIP RRQ.

Usage Guidelines

Use this command to send the PCF address to the HA in a PMIP RRQ.

Example

The following command enables sending the PCF address to the HA in a PMIP RRQ:

```
mobile-ip send pcf-address
```

mobile-ip send service-option

Configures whether the FA sends the service option NVSE in the PMIP RRQ.

Product

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

HA

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > **context** *context_name* > **subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

mobile-ip send service-option [custom-2]

[default | no] mobile-ip send service-option

default

Disables the support for sending the service option to the HA in a PMIP RRQ.

This is the default mode.

no

Removes the configured support for sending the service option to the HA in a PMIP RRQ.

custom-2

NVSE to send service option attribute in the PMIP RRQ.

Usage Guidelines

Use this command to send the service option to the HA in a PMIP RRQ.

Example

The following command enables sending the service option to the HA in a PMIP RRQ:

```
mobile-ip send service-option
```

mobile-ip send subnet-id

Configures whether the FA sends the subnet-id NVSE in the PMIP RRQ.

Product



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

HA

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-subscriber)#`

Syntax Description

```
mobile-ip send subnet-id [ custom-2 ]
[ default | no ] mobile-ip send subnet-id
```

default

Disables the support for sending the subnet-id to the HA in a PMIP RRQ.

This is the default mode.

no

Removes the configured support for sending the subnet-id to the HA in a PMIP RRQ.

custom-2

NVSE to send subnet-id attribute in the PMIP RRQ.

Usage Guidelines

Use this command to send the subnet-id to the HA in a PMIP RRQ.

Example

The following command enables sending the subnet-id to the HA in a PMIP RRQ:

```
mobile-ip send subnet-id
```

mobile-ipv6

Configures Mobile IPv6 related parameters for a subscriber.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

[default | no] mobile-ipv6 { home-address *ipv6_address* **| home-agent** *ipv6_address* **| home-link-prefix** *ipv6_address* **| tunnel mtu** *value* **}**

default

Disables the support for sending call correlation information NVSEs to the HA in MIP RRQ.

This is the default mode.

no

Removes the configured support for sending call correlation information.

home-address *ipv6_address*

Specifies the home address for the subscriber. *ipv6_address* must be entered using IPv6 colon-separated-hexadecimal notation.

home-agent *ipv6_address*

Specifies the IPv6 address of the mobile IP user's home agent. *ipv6_address* must be entered using IPv6 colon-separated-hexadecimal notation.

home-link-prefix *ipv6_address*

Specifies the IPv6 address of the mobile IP user's home link. *ipv6_address* must be entered using IPv6 colon-separated-hexadecimal notation.

tunnel mtu *value*

Configures the tunnel MTU (in bytes) for the IPv6 tunnel between the HA and the mobile node. *value* must be an integer from 1024 through 2000. The default is 1500.

Usage Guidelines

This command sets the mobile-ipv6 parameters for a subscriber. Use this command to set the home-address, home-agent, and home-link prefix

Example

Use the following command to set the tunnel MTU value to *1800*:

```
mobile-ipv6 tunnel mtu 1800
```

nai-construction-domain

After authentication, the domain name specified by this command replaces the Network Access Identifier (NAI) constructed for the subscriber.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-subscriber)#`

Syntax Description

`nai-construction-domain` *`domain_name`*

`no nai-construction-domain`

nai-construction-domain *domain_name*

Defines the domain name to use to replace the NAI constructed domain name. *domain_name* must be an alphanumeric string of 1 through 79 characters.

no

Deletes the defined domain name.

Usage Guidelines

Define or delete a domain name to use to replace the NAI constructed domain name after authentication.

Example

the following command sets the domain name to *private1*:

`nai-construction-domain private1`

To delete the previously configured domain name, use the following command:

`no nai-construction-domain`

nbns

Configures and enables use of NetBIOS Name Service (NBNS) for the subscriber.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > **context** *context_name* > **subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

[no] nbns { primary *IPv4-address* **| secondary** *IPv4-address* **}**

nbns primary

Designates primary NBNS server. Must be followed with IPv4 address in dotted-decimal notation.

nbns secondary

Designates secondary/failover NBNS server. Must be followed with IPv4 address in dotted-decimal notation.

IPv4-address

Specifies the IP address used for this service using IPv4 dotted-decimal notation.

no

Removes/disables use of a previously configured NetBios Name Service.

Usage Guidelines

This command specifies NBNS parameters. The NBNS option is present for both PDP type IP and PDP type PPP for GGSN.

The system can be configured to use of NetBIOS Name Service for the Access Point Name (APN).

Example

The following command configures the subscriber's NetBIOS Name Service to primary IP *192.168.1.15*:

```
nbns primary 192.168.1.15
```

nexthop-forwarding-address

Configures the next hop forwarding address for the subscriber.

Product

PDSN

GGSN

ASN-GW

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > **context** *context_name* > **subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

nexthop-forwarding-address *ip_address*

no nexthop-forwarding-address

nexthop-forwarding-address *ip_address*

Configures the IP address of the nexthop forwarding address. *ip_address* must be entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

no

Disables this function. This is the default setting.

Usage Guidelines

Use this command to configure the next hop forwarding address for the subscriber.

Example

The following command configures the next hop forwarding address to *209.165.200.225* (IPv4):

```
nexthop-forwarding-address 209.165.200.225
```

npu qos

Configures an Network Processing Unit (NPU) QoS priority queue for packets from the subscriber.

Product

PDSN

GGSN

ASN-GW

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > **context** *context_name* > **subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

npu qos traffic priority { best-effort | bronze | derive-from-packet-dscp | gold | silver }

best-effort

Assigns the best-effort queue priority. This is the lowest priority.

bronze

Assigns the bronze queue priority. This is the third-highest priority.

derive-from-packet-dscp

Default: Enabled

Specifies that the priority is to be determined from the DS field in the packet's TOS octet.

gold

Assigns the gold queue priority. This is the highest priority.

silver

Assigns the silver queue priority. This is the second-highest priority.

Usage Guidelines

This command is used in conjunction with the Network Processing Unit (NPU) Quality of Service (QoS) functionality.

The system can be configured to determine the priority of a subscriber packet either based on the configuration of the subscriber, or from the differentiated service (DS) field in the packet's TOS octet (representing the differentiated service code point (DSCP) value).

Refer to the *System Administration Guide* for additional information on NPU QoS functionality.



Important This functionality is not supported for use with the PDSN at this time.

Example

The following command configures the subscriber's priority queue to be gold:

```
npu qos traffic priority gold
```

nw-reachability-server

Binds the name of a configured network reachability server to the current subscriber and enables network reachability detection.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

nw-reachability server *server_name*

no nw-reachability server

nw-reachability server *server_name*

Specifies the name of a network reachability server that has been defined in the current context. *server_name* is an alphanumeric string of 1 through 16 characters.

no nw-reachability server

Deletes the name of the network reachability server from the current subscribers configuration and disable network reachability failure detection for the current subscriber.

Usage Guidelines

Use this command to define the network reachability server for the current subscriber and enable network reachability failure detection for the current subscriber. If a network reachability server is defined in an IP pool, that setting takes precedence over this command.

Important Refer to the HA configuration mode command **policy nw-reachability-fail** to configure the action that should be taken when network reachability fails.

Important Refer to the context configuration mode command **nw-reachability server** to configure network reachability servers.

Important Refer to the **nw-reachability server server_name** keyword of the **ip pool** command in the *Context Configuration Mode Commands* chapter to bind the network reachability server to an IP pool.

Example

To bind a network reachability server named *InternetDevice* to the current subscriber, enter the following command:

```
nw-reachability server InternetDevice
```

outbound

Configures the subscriber host password for use when authenticating PPP sessions.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > **context** *context_name* > **subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

outbound [encrypted] password *pwd*

no outbound password

[outbound encrypted] password *pwd*

Specifies the password to use for point-to-point protocol session host authentication. The **encrypted** keyword indicates the password specified uses encryption.

The password specified as *pwd* must be an alphanumeric string of 1 through 63 characters without encryption, or 1 through 127 characters with encryption.

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 **password** keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

no outbound password

Clears the outbound password configuration from the subscriber data.

Usage Guidelines

Sets the outbound (egress) password for increased security.

Example

```
outbound password secretPwd
outbound encrypted password scrambledPwd
no outbound password
```

overload-disconnect

Sets the threshold parameter for overload disconnect.

Product

ASN-GW

HA

PDIF

PDSN

PHSGW

PDG/TTG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

overload-disconnect [threshold { inactivity-time *inactivity_time_threshold* **| connect-time** *connect_time_threshold* **}]**

[default | no] overload-disconnect [threshold { inactivity-time | threshhold connect-time }]

threshold inactivity-time *inactivity_time_threshold*

Sets the inactivity time threshold (in seconds) as an integer from 0 through 4294967295. The default value of zero disables this feature. If *inactivity-time* for the subscriber's session is greater than *inactivity_time_threshold*, the session becomes a candidate for disconnection.

threshold connect-time *connect_time_threshold*

Sets the connection time threshold (in seconds) as an integer from 0 through 4294967295. A value of zero disables this feature. If connect-time for the subscriber's session is greater than *connect_time_threshold*, the session becomes a candidate for disconnection.

default

Enables the default condition for this subscriber.

no

Disables the overload disconnect feature for this subscriber. This is the default condition for PDIF.

Usage Guidelines

Set a subscriber's overload disconnect threshold in seconds, based on either inactivity or connection time. When this threshold is exceeded during a session, the subscriber's session becomes a candidate for disconnection. To set overload-disconnect policies for the entire chassis, see **congestion-control overload-disconnect** in the *Global Configuration Mode Commands* chapter.

Example

```
overload-disconnect threshold inactivity-time 120
default overload disconnect threshold connect-time
no overload-disconnect threshold connect-time
no overload disconnect
```

password

Configures the subscribers password for the current context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

[encrypted] password *pwd*

no password

encrypted

Indicates the password provided is encrypted.

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 **password** keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

pwd

Specifies the user's password for authentication. *pwd* must be an alphanumeric string of 1 through 63 characters without encryption, or from 1 through 127 characters with encryption. A "null" password is allowed and is entered as consecutive double quotes (" "). See Example(s) for correct syntax.

Important Subscribers configured with a null password will be authenticated using PAP and CHAP (MD5) only. Subscribers configured without a password (**no password**) will only be able to access services if the service is configured to allow no authentication.

no

Used to clear the subscriber password configuration from the subscriber data.

Important Subscribers with no password will only be able to access services if the service is configured to grant access with no authentication.

Usage Guidelines

Password management is critical to system security and all precautions should be taken to ensure passwords are not shared or to easily deciphered.

Example

password *secretPwd*

password ""

```
no password
```

pdif mobile-ip

Configures PDIF subscriber call setup parameters.

Product

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

[default | no] pdif mobile-ip { release-tia | required | simple-ip-fallback }

[default | no]

Disables the option specified.

release-tia

Specifies that after subscriber call setup is complete, the tunnel inner address (TIA) is released. If SImple IP is enabled, the TIA becomes the principal communications tunnel and the restriction that it is only to be used to set up a Mobile-IP call is lifted. This parameter is disabled by default.

required

Specifies that Mobile IP is required for this subscriber whenever a call is set up. This parameter is disabled by default.

simple-ip-fallback

Specifies that Simple IP should be used when Mobile IP could not be established. This parameter is disabled by default.

Usage Guidelines

Use this command to configure specific behavior for the PDIF subscriber during call setup.

Example

The following command enables the system to fall back to Simple IP when Mobile IP fails for this subscriber during call setup:

```
pdif mobile-ip simple-ip-fallback
```

permission

Enables or disables the subscriber's ability to access wireless data services.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

[no] permission { ha-mobile-ip | pdsn-mobile-ip | pdsn-simple-ip | pmipv6-interception }

default permission

no | default

Disables the usage of the specified service.

ha-mobile-ip | pdsn-mobile-ip | pdsn-simple-ip

ha-mobile-ip: Enables or disables the Home Agent (HA) support for Mobile IP (MIP) service.

pdsn-mobile-ip: Enables or disables packet data and Foreign Agent (FA) support for MIP service.

pdsn-simple-ip: Enables or disables packet data support for simple IP service.

pmipv6-interception: Allows subscribers to access the external Local Mobility Anchor (LMA) over PMIPV6.

Usage Guidelines

Grants the subscriber access to services in the current context.

Example

The following command Grants the subscriber access to PDSN/HA services:

permission pdsn-mobile-ip

policy ipv6 tunnel

Sets maximum transmission unit (MTU) behavior for the IPv6 tunnel between the HA and Mobile Node.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-subscriber)#`

Syntax Description

policy ipv6 tunnel mtu exceed { fragment | notify-sender }

mtu exceed { fragment | notify-sender }

fragment: Adjusts tunnel MTU for fragmented packets

notify-sender: Sends an ICMPv6 Packet Too Big message to the original sender

Usage Guidelines

Use this command to configure MTU behavior for an IPv6 tunnel between the HA and Mobile Node.

Example

The following command configures adjustments to tunnel MTU for fragmented packets:

policy ipv6 tunnel mtu exceed fragment

policy-group

Assigns or removes a flow-based traffic policy group to a subscriber.

Product

PDSN

HA

ASN-GW

HSGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-subscriber)#`

Syntax Description

[no] policy-group *policy_group_name* **direction { in | out }**

no

Removes assigned policy group from a subscriber configuration.

policy-group *policy_group_name*

Specifies the traffic policy group name for a subscriber session flow pre-configured within a destination context. *policy_group_name* is an alphanumeric string of 1 through 15 characters that is case sensitive.

direction { in | out }

Specifies the direction of flow in which the traffic policies need to be applied.

- **in**: specifies the incoming traffic
- **out**: specifies the outgoing traffic

Usage Guidelines Use this command to assign a traffic policy group to a subscriber for traffic policing.

Example

The following command assigns inbound traffic policy group *tp-group1* to this subscriber:

```
policy-group tp-group1 direction in
```

ppp

Configures the point-to-point protocol (PPP) options for the current subscriber.

Product PDSN

PDSN Closed R-P

GGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

```
ppp { accept-peer-ipv6-ifid | always-on-vse-packet | data-compression {
mode { normal | stateless } | protocols { protocols [ protocols ] } |
ip-header-compression negotiation { detect | force | vj compress-slot-id
 { both | none | receive | transmit } } | ipv4 { disable | enable | passive
 } | ipv6 { disable | enable | passive } | keepalive seconds |
min-compression-size min_octets | mtu max_octets | remote-renegotiation
disconnect { always | nai-prefix-msid-mismatch } }
```

```
default ppp { accept-peer-ipv6-ifid | always-on-vse-packet |
data-compression { mode | protocols } | ip-header-compression negotiation
 [ vj compress-slot-id ] | ipv4 | ipv6 | keepalive | min-compression-size
 | mtu | remote-renegotiation disconnect }
```

```
no ppp { accept-peer-ipv6-ifid | always-on-vse-packet | data-compression
 protocols | ipv4 | ipv6 | keepalive | mtu | remote-renegotiation
disconnect }
```

default

Restores the default value for the option specified.

no

Resets the option specified to its default.

always-on-vse-packet

Default: Enabled

If this feature is enabled, the PDSN sends special 3GPP2 VSE PPP packets to the Mobile Node with a maximum inactivity timer value. This configuration is applicable only for PDSN or PDSNCLOSED-RP sessions.

accept-ipv6-peer-ifield

Default: None

Configures an IPv6-to-IPv4 (6to4) tunnel and controls the behavior of IPv6CP negotiation for the Interface ID. If enabled, PDSN will accept a valid interface-id proposed by the peer.

data-compression { mode { normal | stateless } | protocols { *protocols* [*protocols*] }

Default: all protocols enabled.

Specifies the subscriber's mode of data compression or the compression protocol to use.

mode: sets the mode of compression where *modes* must be one of:

- **normal**: Packets are compressed using the packet history for automatic adjustment for best compression.
- **stateless**: Each packet is compressed individually.

protocols *protocols*: sets the compression protocol where *protocols* must be one of:

- **deflate**: DEFLATE algorithm
- **mppc**: Microsoft PPP algorithm
- **stac**: STAC algorithm

ip-header-compression negotiation { detect | force | vj compress-slot-id { both | none | receive | transmit } }

Default: **force**

detect: The local side does not include the Van Jacobson (VJ) Compression option in its IPCP configuration request unless the peer sends an Internet Protocol Control Protocol (IPCP) NAK including a VJ compression option. If the peer requests the VJ compression option in its IPCP request the local side will ACK/NAK.

force: The IP header compression negotiation in IPCP happens normally. The local side requests the VJ compression option in its IPCP configure request. If the peer side requests VJ compression in its IPCP request, the local side will ACK/NAK the option.

vj compress-slot-id [both | none | receive | transmit]: Configures the direction in which VJ slotid compression should be negotiated.

- **both** - If the client proposes VJ slotid compression, accept it and propose slotid compression for the downlink and uplink.
- **none** - If the client proposes VJ slotid compression, NAK the offer, do not propose slotid compression for the downlink.
- **receive** - (Default) If the client proposes VJ slotid compression in the uplink direction accept the configuration.
- **transmit** - Propose VJ slotid compression for uplink.

ipv4 { disable | enable | passive }

Default: enable

Controls IPCP negotiation during PPP negotiation.

disable: The PDSN does not negotiate IPCP with the mobile.

enable: The PDSN negotiates IPCP with the mobile.

passive: The PDSN initiates IPCP only when the mobile sends an IPCP request.

ipv6 { disable | enable | passive }

Default: enable

Controls IPv6CP negotiation during PPP negotiation.

disable: The PDSN does not negotiate IPCP with the mobile.

enable: The PDSN negotiates IPCP with the mobile.

passive: The PDSN initiates IPCP only when the mobile sends an IPCP request.

keepalive *seconds*

Default: 30

Specifies the frequency of sending the Link Control Protocol keepalive messages. *seconds* must be either 0 or an integer from 5 through 14400. The special value 0 disables the keepalive messages entirely.

min-compression-size *min_octets*

Default: 128

Specifies the smallest packet (in octets) to which compression may be applied. *min_octets* must be an integer from 0 through 2000.

mtu *max_octets*

Default: 1500

Specifies the maximum transmission unit (MTU) [in octets] for packets. *max_octets* must be an integer from 100 through 2000.

remote-renegotiation disconnect { always | nai-prefix-msid-mismatch }

Default: Disabled

Terminates the already established PPP sessions if they are renegotiated by the remote side by sending LCP Conf-req/nak/ack. The following termination conditions are available:

- **always**: Automatically disconnects the session.
- **nai-prefix-msid-mismatch**: Disconnects the session only if the MSID of the session does not match NAI-Prefix (prefix before "@" for the NAI). The configuration of the renegotiated (new) NAI is used for the matching process.

Usage Guidelines

Adjust packet sizes and compression to improve bandwidth utilization. Each network may have unique characteristics such that determining the best packet size and compression options may require system monitoring over an extended period of time.

Example

The following sequence of CLI commands sets PPP parameters for this subscriber:

```
ppp data-compression protocols mode stateless
ppp mtu 500
no ppp data-compression protocols
no ppp keepalive
```

prepaid 3gpp2

Enables 3GPP2 compliant prepaid billing support for a subscriber to be configured by 3GPP2 attributes sent from a RADIUS server. If not enabled, prepaid attributes received from the RADIUS server are ignored.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

```
prepaid 3gpp2 { accounting [ no-final-access-request ] | duration-quota
final-duration-algorithm { current-time | last-airlink-activity-time |
last-user-layer3-activity-time } | preference { duration | volume } }
default prepaid 3gpp2 { duration-quota final-duration-algorithm |
preference }
no prepaid 3gpp2 accounting
```

default prepaid 3gpp2 { duration-quota final-duration-algorithm | preference }

Sets the 3GPP2 Pre-paid settings to the default values.

duration-quota final-duration-algorithm: Resets the end of billing duration quota algorithm to the default of current-time.

preference: Resets the preference to duration, If both duration and volume attributes are present.

no prepaid 3gpp2 accounting

Disables 3GPP2 prepaid accounting. All 3GPP2 Prepaid attributes received from a RADIUS server are ignored.

accounting [no-final-access-request]

Default: Disabled

Enables 3GPP2 prepaid accounting behavior.

Sets the low-watermark for remaining byte credits. *percentage* is a percentage of the subscriber sessions total credits. When the low-watermark is reached a new RADIUS access-request is sent to the RADIUS server to retrieve more credits. *percentage* must be an integer from 1 through 99.

no-final-access-request: Stops sending final online access-request on termination of 3GPP2 prepaid sessions. By default, this option is disabled.

duration-quota final-duration-algorithm { current-time | last-airlink-activity-time | last-user-layer3-activity-time }

Defines what behavior marks the end of the billing duration for duration-based quota usage accounting. The default behavior sets the duration quota algorithm to current-time.

Default: current-time

current-time: Selects the duration quota as the difference between the session termination timestamp and the session setup timestamp.

last-airlink-activity-time: Selects the duration quota as the difference between the last-user-activity timestamp (G17) and the session setup timestamp.

last-user-layer3-activity-time: Selects the duration quota as the difference between the timestamp of the last layer-3 packet sent to or received from the user and the session setup timestamp.

preference { duration | volume }

If both duration and volume RADIUS attributes are present this keyword specifies which attribute has precedence.

Default: duration

duration: The duration attribute takes precedence.

volume: The volume attribute takes precedence

Usage Guidelines

Use this command to enable prepaid support for a default user or for the default user of a domain alias.

Example

The following command enables 3GPP2 prepaid support for the default user:

```
prepaid 3gpp2 accounting
```

prepaid custom

Enables custom prepaid billing support for a subscriber to be configured by attributes sent from a RADIUS server. If not enabled, prepaid attributes received from the RADIUS server are ignored. The keywords set prepaid values that are used if the corresponding RADIUS attribute is not present. If the RADIUS attribute is present, it takes precedence over these values.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

prepaid custom { accounting | byte-count compressed | low-watermark percent *percentage* **| renewal interval** *seconds* **} | preference { duration | volume }**

default prepaid custom { byte-count | low-watermark }

no prepaid custom { accounting | byte-count compressed | low-watermark | renewal }

default prepaid custom { byte-count | low-watermark }

Resets custom prepaid settings to the default values.

byte-count: Resets to the default of basing the prepaid byte credits on the flow of uncompressed traffic.

low-watermark: Disables sending an access request to retrieve more credits when a low watermark is reached.

no prepaid custom { accounting | byte-count compressed | low-watermark | renewal}

byte-count compressed: The prepaid byte credits are based on the flow of uncompressed traffic. This is the default.

low-watermark: Disables the low watermark feature. An access-request is not sent to the RADIUS server until the credits granted for the subscriber session are depleted.

renewal: Disables time-based renewals for prepaid accounting.

accounting

Default: Disabled

Enables custom prepaid accounting behavior.

byte-count compressed

Default: uncompressed.

When compression is used, the prepaid byte credits are based on the flow of compressed traffic. The default is to base the prepaid byte credits on the flow of uncompressed traffic.

low-watermark percent *percentage*

Default: Disabled.

Sets the low-watermark for remaining byte credits. *percentage* is a percentage of the subscriber sessions total credits. When the low-watermark is reached a new RADIUS access-request is sent to the RADIUS server to retrieve more credits. *percentage* must be an integer from 1 through 99.

renewal interval *seconds*

Default:

The time in seconds to wait before sending a new RADIUS access-request to the RADIUS server to retrieve more credits. *seconds* must be an integer from 60 through 65535.

preference { duration | volume }

If both duration and volume RADIUS attributes are present this keyword specifies which attribute has precedence.

Default: duration

duration: The duration attribute takes precedence.

volume: The volume attribute takes precedence

Usage Guidelines

Use this command to enable prepaid support for a default user or for the default user of a domain alias.

Example

The following command enables custom prepaid support for the default user:

```
prepaid custom accounting
```

prepaid unclassify

This command provides customer specific functionality.

prepaid voice-push

This command provides customer specific functionality.

prepaid wimax

Enables WiMAX prepaid accounting for this subscriber. This feature is disabled by default.

Product

ASN-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-subscriber)#`

Syntax Description

`[ no ] prepaid wimax accounting`

no

Disables WiMAX prepaid accounting for this subscriber.

Usage Guidelines

Use this command to enable WiMAX prepaid accounting for this subscriber.

Example

The following command enables WiMAX prepaid accounting for this subscriber:

`prepaid wimax accounting`

proxy-dns intercept list-name

Identifies a proxy DNS intercept rules list for the selected subscriber.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-subscriber)#`

Syntax Description **`[ no ] proxy-dns intercept list-name`** *`name`*

no

Removes the intercept list from the subscribers profile.

proxy-dns intercept list-name *name*

Specifies a name of a proxy DNS intercept list used for the selected subscriber.

name is the name of the intercept list expressed as an alphanumeric string of 1 through 63 characters.

Usage Guidelines Use this command to identify a proxy DNS rules list for the selected subscriber. For a more detailed explanation of the HA Proxy DNS Intercept feature, see the **proxy-dns intercept-list** command in the *Context Configuration Mode Commands* chapter.

Example

The following command specifies the proxy DNS intercept list named *dns-Intercept-list*:

```
proxy-dns intercept list-name dns-Intercept-list
```

proxy-mip

Configures support for Proxy Mobile IP for the subscriber.

Product PDSN

GGSN

ASN-GW

PDIF

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description **`[ no ] proxy-mip required`**

no

Disables support for Proxy Mobile IP.

required

Enables support for Proxy Mobile IP.

Usage Guidelines

When enabled through the session license and feature use key, the system supports Proxy Mobile IP to provide a mobility solution for subscribers with mobile nodes (MNs) capable of supporting only Simple IP.

For subscriber sessions using Proxy Mobile IP, R-P and PPP sessions are established as they would for a Simple IP session. However, the AGW/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber's profile) on behalf of the MN while the MN performs only Simple IP processes.

Example

The following command enables proxy mobile IP for the current subscriber:

```
proxy-mip required
```

qos apn-ambr

Configures the rate limit according to the APN-AMBR to do the session level bandwidth control per direction, according to the QoS information provided by the PCRF on the Gx interface.

Product

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

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

qos apn-ambr rate-limit { **downlink** | **uplink** } [**burst-size** *bytes*] [**violate-action** { **drop** | **lower-ip-precedence** | **transmit** }]]

no qos apn-ambr rate-limit

no

Disables the QoS data rate limit configuration for the subscriber.

downlink

Applies the specified limits and actions to the downlink (to the data coming from the GGSN over the Gn' interface).

uplink

Applies the specified limits and actions to the uplink (to the data coming from the UE over the IPSec tunnel).

Important If this keyword is omitted, the same values are used for all classes.

burst-size *bytes*

Default: See the *Usage* section for this command

The burst size allowed (in bytes) for peak data rate and committed data rate.

bytes must be an integer from 1 through 6000000.

Important The minimum value of this parameter should be configured to the greater of the following two values: 1) three times greater than the packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the "bucket" for the configured peak-data-rate. If the committed-data-rate parameter is specified, the burst-size is applied to both the committed and peak rates.

violate-action { drop | lower-ip-precedence | transmit }

Default: See the *Usage* section for this command

Specifies the action to take on packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:

- **drop**: Drops the packets.
- **lower-ip-precedence**: Transmits the packets after lowering the IP precedence.
- **transmit**: Transmits the packet.

Usage Guidelines This command configures the rate limit according to the APN-AMBR to do the session level bandwidth control per direction, according to the QoS information provided by the PCRF on the Gx interface. This command specifies the actions to take on subscriber flows exceeding or violating allowed peak or committed data rates.

Example

The following example configures the rate limit and burst size according to the APN-AMBR for the uplink direction. Policing is done for the traffic based on PCRF value recieved and traffic is dropped as the violate action is specified as drop.

```
qos apn-ambr rate-limit direction uplink burstsize 1 violate-action drop
```

qos rate-limit

Configure the action on subscriber traffic flow that violates or exceeds the peak/committed data rate under traffic policing functionality. When configured, the PDG/TTG performs traffic policing for the subscriber session. If the GGSN changes the QoS via an Update PDP Context Request, the PDG/TTG uses the new QoS values for traffic policing.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

qos rate-limit { **downlink** | **uplink** } [**qci** *qci_val*] [**burst-size** { *bytes* | **auto-readjust** [**duration** *dur*] }] [**exceed-action** { **drop** | **lower-ip-precedence** | **transmit** } [**violate-action** { **drop** | **lower-ip-precedence** | **shape** [**transmit-when-buffer-full**] | **transmit** }]] | [**violate-action** { **drop** | **lower-ip-precedence** | **shape** [**transmit-when-buffer-full**] | **transmit** } [**exceed-action** { **drop** | **lower-ip-precedence** | **transmit** }]] +

no qos rate-limit direction { downlink | uplink } [**qci** *qci_val*]

no

Disables the QoS data rate limit configuration for the subscriber.

downlink

Applies the specified limits and actions to the downlink (to the data coming from the GGSN over the Gn' interface).

uplink

Applies the specified limits and actions to the uplink (to the data coming from the UE over the IPSec tunnel).



Important If this keyword is omitted, the same values are used for all classes.

qci *qci_val*

qci_val is the QoS Class identifier (QCI) for which the negotiate limit is being set expressed as an integer from 1 through 9. If no qci-val is configured, it will be taken as undefined-qci (same as undefined-qos class).

burst-size { *bytes* | auto-readjust [duration *dur*] }

Default: See the *Usage* section for this command

The burst size allowed (in bytes) for peak data rate and committed data rate.

bytes must be an integer from 1 through 6000000.



Important The minimum value of this parameter should be configured to the greater of the following two values: 1) three times greater than the packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the "bucket" for the configured peak-data-rate. If the committed-data-rate parameter is specified, the burst-size is applied to both the committed and peak rates.

auto-readjust [duration *dur* **]** provides the option to calculate the Burst size dynamically while configuring rate-limit. When enabled. the system calculates the burst size using the GGSN QoS-negotiated rate that will be enforced.

Every time there is a change in the rates (due to an updated QoS), the burst sizes will be updated accordingly.

This keyword also provides two different burst sizes. One burst size for peak rate and another for committed rate.

By default this keyword is disabled.

duration *dur* specifies the duration of burst in seconds. If the duration is not specified, the default is 1 second. *dur* must be an integer from 1 through 30.

exceed-action { drop | lower-ip-precedence | transmit }

Default: See the *Usage* section for this command

Specifies the action to take on packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:

- **drop**: Drops the packets.
- **lower-ip-precedence**: Transmits the packets after lowering the ip-precedence.
- **transmit**: Transmits the packets.

violate-action { drop | lower-ip-precedence | transmit }

Default: See the *Usage* section for this command

Specifies the action to take on packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:

- **drop**: Drops the packets.
- **lower-ip-precedence**: Transmits the packets after lowering the IP precedence.
- **transmit**: Transmits the packet after lowering the IP precedence.

shape [transmit-when-buffer-full]: Enables traffic shaping and buffers user packets when subscriber traffic violates the allowed peak/committed data rate. The **[transmit-when-buffer-full]** keyword allows the packets to be transmitted when buffer memory is full.

transmit: Transmits the packet

Usage Guidelines

This command configures APN quality of service (QoS) data rate shaping through traffic policing. This command specifies the actions to take on subscriber flows exceeding or violating allowed peak or committed data rates. The shaping function also provides an enhanced function to buffer the excessive user packets and send them to the subscriber when subscriber traffic drops below the committed or peak data rate limit.

Important The buffering of user packets in traffic shaping does not apply for real-time traffic.

Important If the exceed/violate action is set to "lower-ip-precedence", this command may override the configuration of the **ip qos-dscp** command in the GGSN service Configuration mode for packets from the GGSN to the PDG/TTG. In addition, the GGSN service **ip qos-dscp** command configuration can override the APN setting for packets from the GGSN to the Internet. Therefore, it is recommended that this command not be used in conjunction with this action.

The command can be entered multiple times to specify different combinations of direction and class. If this command is not configured at all, the GGSN does not perform traffic policing or QoS negotiation with the PDG/TTG; it accepts all of the PDG/TTG-provided values for the PDP context.

Important This command should be used in conjunction with the max-contexts command to limit the maximum possible bandwidth consumption by the APN.

For additional information on QoS traffic shaping and policing, see the *System Administration Guide.*

Default Values

The following table displays the default values for each of the traffic classes:

Class: Conversational	
Downlink Traffic: Disabled Peak Data Rate (in bps): 16000000 Committed Data Rate (in bps): 16000000 Exceed Action: lower-ip-precedence Violate Action: drop	Uplink Traffic: Disabled Peak Data Rate (in bps): 8640000 Committed Data Rate (in bps): 8640000 Exceed Action: lower-ip-precedence Violate Action: drop
Class: Streaming	
Downlink Traffic: Disabled Peak Data Rate (in bps): 16000000 Committed Data Rate (in bps): 16000000 Exceed Action: lower-ip-precedence Violate Action: drop	Uplink Traffic: Disabled Peak Data Rate (in bps): 8640000 Committed Data Rate (in bps): 8640000 Exceed Action: lower-ip-precedence Violate Action: drop
Class: Interactive, Traffic Handling Priority: 1	

Downlink Traffic: Disabled Peak Data Rate (in bps): 16000000 Committed Data Rate (in bps): n/a Exceed Action: n/a Violate Action: drop	Uplink Traffic: Disabled Peak Data Rate (in bps): 8640000 Committed Data Rate (in bps): n/a Exceed Action: n/a Violate Action: drop
Class: Interactive, Traffic Handling Priority: 2	
Downlink Traffic: Disabled Peak Data Rate (in bps): 16000000 Committed Data Rate (in bps): n/a Exceed Action: n/a Violate Action: drop	Uplink Traffic: Disabled Peak Data Rate (in bps): 8640000 Committed Data Rate (in bps): n/a Exceed Action: n/a Violate Action: drop
Class: Interactive, Traffic Handling Priority: 3	
Downlink Traffic: Disabled Peak Data Rate (in bps): 16000000 Committed Data Rate (in bps): n/a Exceed Action: n/a Violate Action: drop	Uplink Traffic: Disabled Peak Data Rate (in bps): 8640000 Committed Data Rate (in bps): n/a Exceed Action: n/a Violate Action: drop
Class: Background	
Downlink Traffic: Disabled Peak Data Rate (in bps): 16000000 Committed Data Rate (in bps): n/a Exceed Action: n/a Violate Action: drop	Uplink Traffic: Disabled Peak Data Rate (in bps): 8640000 Committed Data Rate (in bps): n/a Exceed Action: n/a Violate Action: drop

Usage Guidelines

This command configures the APN quality of service (QoS) data rate shaping through traffic policing/shaping. This command specifies the actions to take on subscriber flows exceeding or violating allowed peak/committed data rates. The shaping function also provides an enhanced function to buffer the excessive user packets and send them to the subscriber when subscriber traffic drops below the committed or peak data rate limit.

Important The buffering of user packets in traffic shaping does not apply for real-time traffic.

Important If the exceed/violate action is set to "lower-ip-precedence", this command may override the configuration of the **ip qos-dscp** command in the GGSN service configuration mode for packets from the GGSN to the SGSN. In addition, the GGSN service **ip qos-dscp** command configuration can override the APN setting for packets from the GGSN to the Internet. Therefore, it is recommended that command not be used in conjunction with this action.

The command can be entered multiple times to specify different combinations of direction and class. If this command is not configured at all, the GGSN does not perform traffic policing or QoS negotiation with the SGSN (i.e. it accepts all of the SGSN-provided values for the PDP context.

Important This command should be used in conjunction with the **max-contexts** command to limit the maximum possible bandwidth consumption by the APN.

For additional information on QoS traffic shaping and policing, see the *System Administration Guide*.

Default Values:

The following table displays the default values for each of the traffic classes:

Table 1: no title 754

Class: Conversational	
Downlink Traffic: Disabled Peak Data Rate (in bps): 16000000 Committed Data Rate (in bps): 16000000 Burst Size (in bytes): 65535 Exceed Action: lower-ip-precedence Violate Action: drop	Uplink Traffic: Disabled Peak Data Rate (in bps): 8640000 Committed Data Rate (in bps): 8640000 Burst Size (in bytes): 65535 Exceed Action: lower-ip-precedence Violate Action: drop
Class: Streaming	
Downlink Traffic: Disabled Peak Data Rate (in bps): 16000000 Committed Data Rat (in bps): 16000000 Burst Size (in bytes): 65535 Exceed Action: lower-ip-precedence Violate Action: drop	Uplink Traffic: Disabled Peak Data Rate (in bps): 8640000 Committed Data Rate (in bps): 8640000 Burst Size (in bytes): 65535 Exceed Action: lower-ip-precedence Violate Action: drop
Class: Interactive, Traffic Handling Priority: 1	

Downlink Traffic: Disabled Peak Data Rate (in bps): 16000000 Committed Data Rate (in bps): n/a Burst Size (in bytes): 65535 Exceed Action: n/a Violate Action: drop	Uplink Traffic: Disabled Peak Data Rate (in bps): 8640000 Committed Data Rate (in bps): n/a Burst Size (in bytes): 65535 Exceed Action: n/a Violate Action: drop
Class: Interactive, Traffic Handling Priority: 2	
Downlink Traffic: Disabled Peak Data Rate (in bps): 16000000 Committed Data Rate (in bps): n/a Burst Size (in bytes): 65535 Exceed Action: n/a Violate Action: drop	Uplink Traffic: Disabled Peak Data Rate (in bps): 8640000 Committed Data Rate (in bps): n/a Burst Size (in bytes): 65535 Exceed Action: n/a Violate Action: drop
Class: Interactive, Traffic Handling Priority: 3	
Downlink Traffic: Disabled Peak Data Rate (in bps): 16000000 Committed Data Rate (in bps): n/a Burst Size (in bytes): 65535 Exceed Action: n/a Violate Action: drop	Uplink Traffic: Disabled Peak Data Rate (in bps): 8640000 Committed Data Rate (in bps): n/a Burst Size (in bytes): 65535 Exceed Action: n/a Violate Action: drop
Class: Background	
Downlink Traffic: Disabled Peak Data Rate (in bps): 16000000 Committed Data Rate (in bps): n/a Burst Size (in bytes): 65535 Exceed Action: n/a Violate Action: drop	Uplink Traffic: Disabled Peak Data Rate (in bps): 8640000 Committed Data Rate (in bps): n/a Burst Size (in bytes): 65535 Exceed Action: n/a Violate Action: drop



Important If a "Subscribed" traffic class is received, the system changes the class to "Background" and sets the following parameters: The uplink and downlink guaranteed data rates are set to 0. If the received uplink or downlink data rates are 0 and traffic policing is disabled, the default of 64 kbps is used. When enabled, the APN configured values are used. If the configured value for downlink max data rate is larger than can fit in an R4 QoS profile, the default of 64 kbps is used. If either the received uplink or downlink max data rates is non-zero, traffic policing is employed if enabled for the "Background" class. The received values are used for responses when traffic policing is disabled.

To calculate the burst size dynamically a new optional keyword **auto-readjust** [**duration** *dur*] is provided with **burst-size** keyword. By default the burst size is fixed if defined in bytes with this command. In other words irrespective of the rate being enforced, burst-size fixed as given in the **burst-size** *bytes* parameter.

For the need of variable burst size depending on the rate being enforced this new keyword **auto-readjust** [**duration** *dur*] is provided. Use of this keyword enables the calculation of burst size as per token bucket algorithm calculation as T=B/R, where T is the time interval, B is the burst size and R is the Rate being enforced.

It also provides different burst size for Peak and Committed data rate-limiting.

If **auto-readjust** keyword is not used a fixed burst size must be defined which will be applicable for peak data rate and committed data rate irrespective of rate being enforced.

If **auto-readjust** keyword is provided without specifying the duration a default duration of 1 second will be taken for burst size calculation.

Example

The following command lowers the IP precedence when the committed-data-rate and the peak-data-rate are violated in uplink direction:

```
qos rate-limit direction uplink violate-action lower-ip-precedence
```

The following command buffers the excess user packets when the subscriber traffic violates the configured peak or committed data-rate bps in uplink direction. Once the peak/committed data rate for that subscriber goes below the configured limit it transmit them. It also transmits them if buffer memory is full:

```
qos rate-limit direction uplink violate-action shape
transmit-when-buffer-full
```

qos traffic-police

Enables and configures traffic policing through bandwidth limitations and action for the subscriber traffic if it exceeds or violates the peak or committed data rate. Uplink and downlink limits are configured separately.

Product

PDSN

HA

GGSN

ASN-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

qos traffic-police direction { downlink | uplink } [burst-size *bytes* **] [committed-data-rate** *bps* **] [exceed-action { drop | lower-ip-precedence | transmit }] [peak-data-rate** *bps* **] [violate-action { drop | lower-ip-precedence | transmit }]**

no qos traffic-police direction { downlink | uplink }

downlink

Applies the specified limits and actions to the downlink (data to the subscriber).

uplink

Apply the specified limits and actions to the uplink (data from the subscriber).

burst-size *bytes*

Default: 3000

Specifies the allowed peak burst size allowed in bytes.

bytes must be an integer from 0 through 4294967295.



Important This parameter should be configured to at least the greater of the following two values: 1) three times greater than packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the "bucket" for the configured peak-data-rate.

committed-data-rate *bps*

Default: 144000

Specifies the committed data rate (guaranteed-data-rate) in bits per second (bps).

bps must be an integer from 0 through 4294967295.

exceed-action { drop | lower-ip-precedence | transmit }

Default: lower-ip-precedence

Specifies the action to take on packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:

drop: Drops the packet

lower-ip-precedence: Transmits the packet after lowering the ip-precedence

transmit: Transmits the packet

peak-data-rate *bps*

Default: 256000

Specifies the peak data-rate for the subscriber in bits per second (bps).

bps must be an integer from 0 through 4294967295.

violate-action { drop | lower-ip-precedence | transmit }

Default: drop

Specifies the action to take on packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:

drop: Drops the packet

lower-ip-precedence: Transmits the packet after lowering the IP precedence

transmit: Transmits the packet

no

Disables traffic policing in the specified direction for the current subscriber.

Usage Guidelines

Use this command to limit the bandwidth a subscriber uses in the uplink and downlink directions.



Important If the exceed/violate action is set to "lower-ip-precedence", the TOS value for the outer packet becomes "best effort" for packets that exceed/violate the traffic limits regardless of what the **ip user-datagram-tos copy** command is configured to. In addition, the "lower-ip-precedence" option may also override the configuration of the **ip qos-dscp** command. Therefore, it is recommended that command not be used when specifying this option.

Details on the QoS traffic policing can be found in the *System Administration Guide*.

Example

The following command sets an uplink peak data rate of *128000* bps and lowers the IP precedence when the committed-data-rate and the peak-data-rate are exceeded:

```
qos traffic-police direction uplink peak-data-rate 128000 violate-action
 lower-ip-precedence
```

The following command sets a downlink peak data rate of *256000* bps and drops packets when the committed-data-rate and the peak-data-rate are exceeded:

```
qos traffic-police direction downlink peak-data-rate 256000 violate-action
 drop
```

qos traffic-shape

Enables and configures traffic shaping functionality when buffering the data packets during congestion or when the subscriber exceeds the configured peak or committed data rate limit. The system buffers the data

packets during an instantaneous burst and deliver them to the subscriber when traffic flow drops below the peak or committed data rate. Uplink and downlink traffic shaping are configured separately.



Important This feature is NOT supported for real-time traffic.

Product

PDSN

HA

GGSN

ASN-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > **context** *context_name* > **subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

qos traffic-shape direction { downlink | uplink } [burst-size *bytes* **] [committed-data-rate** *bps* **] [exceed-action { drop | lower-ip-precedence | transmit }] [peak-data-rate** *bps* **] [violate-action { drop | lower-ip-precedence | buffer [transmit-when-buffer-full] | transmit }] +**

no qos traffic-shape direction { downlink | uplink }

downlink

Applies the specified limits and actions to the downlink (data to the subscriber).

uplink

Applies the specified limits and actions to the uplink (data from the subscriber).

burst-size *bytes*

Default: 3000

Specifies the allowed peak burst size in bytes.

bytes must be an integer from 0 through 4294967295.



Important It is recommended that this parameter be configured to at least the greater of the following two values: 1) three times greater than packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the "bucket" for the configured peak-data-rate.

committed-data-rate *bps*

Default: 144000

Specifies the committed data rate (guaranteed-data-rate) in bits per second (bps).

bps must be an integer from 0 through 4294967295.

exceed-action { drop | lower-ip-precedence | transmit }

Default: lower-ip-precedence

Specifies the action to take on packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:

drop: Drops the packet

lower-ip-precedence: Transmits the packet after lowering the ip-precedence

transmit: Transmits the packet

peak-data-rate *bps*

Default: 256000

Specifies the peak data-rate for the subscriber in bits per second (bps).

bps must be an integer from 0 through 4294967295.

violate-action { drop | lower-ip-precedence | buffer [transmit-when-buffer-full] | transmit }

Default: See the *Usage* section for this command

The action to take on the packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:

drop: Drops the packet

lower-ip-precedence: Transmits the packet after lowering the IP precedence

buffer [transmit-when-buffer-full]: Enables traffic shaping and buffers user packets when subscriber traffic violates the allowed peak/committed data rate. The **[transmit-when-buffer-full]** keyword allows the packet to be transmitted when buffer memory is full.

transmit: Transmits the packet

+

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

no

Disables traffic policing for the specified direction for the current subscriber.

Usage Guidelines

Use this command to provide the traffic shaping function to a subscriber in the uplink and downlink directions. This feature is providing a traffic flow control different to QoS traffic policing. When a subscriber violates or exceeds the peak data rate instead of dropping the packets, as in QoS traffic policing, this feature buffers subscriber data packets and sends the buffered data when the traffic flow is low or not in congestion state.



Important If the exceed or violate action is set to "lower-ip-precedence", the TOS value for the outer packet becomes "best effort" for packets that exceed or violate the traffic limits regardless how the **ip user-datagram-tos copy** command is configured. In addition, the "lower-ip-precedence" option may also override the configuration of the **ip qos-dscp** command. Therefore, this command should not be used when specifying this option.

Details on the QoS traffic policing functionality is located in the System Administration Guide.

Example

The following command sets an uplink peak data rate of *128000* bps and lowers the IP precedence when the committed-data-rate and the peak-data-rate are exceeded:

```
qos traffic-shape direction uplink peak-data-rate 12800 violate-action
lower-ip-precedence
```

The following command buffers the excess user packets when the subscriber traffic violates the configured peak-data-rate *256000* bps in downlink direction. Once the peak/committed data rate for that subscriber goes below the configured limit it transmit them. It also transmits them if buffer memory is full:

```
qos traffic-shape direction downlink peak-data-rate 256000 violate-action
 buffer transmit-when-buffer-full
```

radius accounting

Sets the RADIUS accounting parameters for the subscriber or domain. This command takes precedence over the similar Context Configuration command and is disabled by default.

Product

All

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

```
radius accounting { interim { interval-timeout timeout | normal | suppress
 } | ip remote-address list-id list_id | mode { session-based |
access-flow-based { none | auxillary-flows | all-flows | main-a10-only }
 } | start { normal | suppress } | stop { normal | suppress } }
```

```
no radius accounting { ip remote-address list-id list_id | interim [
interval-timeout ] }
```

interim { interval-timeout *timeout* | normal | suppress }

interval-timeout *timeout*: Indicates the time (in seconds) between updates to session counters (log file on RADIUS or AAA event log) during the session. *timeout* must be an integer from 50 to 40000000.



Caution Interim interval settings received from the RADIUS server take precedence over this setting on the system. While the low limit of this setting on the system is a minimum of 50 seconds, the low limit setting on the RADIUS server can be as little as 1 second. To avoid increasing network traffic unnecessarily and potentially reducing network and system performance, do not set this parameter to a value less than 50 on the RADIUS server.

normal: If RADIUS accounting is enabled, sends this Acct-Status-Type message when required by normal operation

suppress: If RADIUS accounting is enabled, suppresses the sending of this Acct-Status-Type message.

ip remote-address list-id *list_id*

Specifies the identification number of the IP address list to use for the subscriber for remote address-based accounting.

list_id: Specifies the RADIUS accounting remote IP address list identifier for remote-address accounting for the subscriber. *list_id* must be an integer from 1 through 65535.

This command is used as part of the Remote Address-based accounting feature and associates the subscriber with a list of remote addresses. Remote address accounting data is collected each time the subscriber communicates with any of the addresses specified in the list.

Remote address lists are configured using the **list** keyword in the **radius accounting ip remote-address** command in the Context Configuration mode.

mode { session-based | access-flow-based { none | auxillary-flows | all-flows | main-a10-only } }

Default: **session-based**

Specifies if the radius accounting mode is either session-based or access-flow-based.

session-based: configures session-based RADIUS accounting behavior for the subscriber - which means a single radius accounting message generated for the subscriber session not separate accounting messages for individual A10 connections or flows.

access-flow-based: configures access-flow-based RADIUS accounting behavior for the subscriber. This offers flexibility by generating separate accounting messages for flows and A10 sessions.

- **all-flows**: Generates separate RADIUS accounting messages per access flow. Separate accounting messages are not generated for data path connections. (For example, separate messages are not sent for the main A10 or auxiliary connections.).
- **auxillary-flows**: Generates RADIUS accounting records for the main data path connection and for access-flows for all auxiliary data connections. (For example, separate RADIUS accounting messages are generated for the main A10 session and for access-flows within auxiliary A10 connections. The main A10 session accounting does not include octets or other accounting information from the auxiliary flows.)
- **main-a10-only**: Configures access-flow-based single accounting messages (for example only single start/interim/stop) are generated for the main A-10 flows only.

- **none**: Generates separate RADIUS accounting messages for all data path connections (for example, PDSN main or auxiliary A10 connections) but not for individual access-flows. This is essentially A10 connection-based accounting.

start { normal | suppress }

normal: If RADIUS accounting is enabled, sends this Acct-Status-Type message when required by normal operation

suppress: If RADIUS accounting is enabled, suppresses the sending of this Acct-Status-Type message.

stop { normal | suppress }

normal: If RADIUS accounting is enabled, sends this Acct-Status-Type message when required by normal operation

suppress: If RADIUS accounting is enabled, suppresses the sending of this Acct-Status-Type message.

no

ip remote-address list-id *list_id*: Deletes the entry for the specified *list_id.*

interim [interval-timeout]: Disables the interim interval setting.

Usage Guidelines

Use this command to allow a per-domain setting for the RADIUS accounting.

Example

Set the accounting interim interval to one minute (*60* seconds) for all sessions that use the current subscriber configuration:

```
radius accounting interim interval-timeout 60
```

Do not send RADIUS interim accounting messages:

```
radius accounting interim suppress
```

Sets the accounting message start normal for main A-10 flows only.

```
radius accounting mode main-a10-only start normal
```

radius group

Applies a RADIUS server group at the subscriber level for AAA functionality.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

radius group *group_name*

{ default | no } radius group

radius *group_name*

Specifies the name of the server group that is used for authentication and/or accounting for the specific subscriber. *group_name* must be an alphanumeric string of 1 through 63 characters. It must have been preconfigured within the same context of subscriber.

default

Sets or restores the default RADIUS server group specified at the context level or in the default subscriber profile.

no

Disables the applied RADIUS group for specific subscriber.

Usage Guidelines

This feature provides the RADIUS configurables under radius group node. Instead of having a single list of servers per context, this feature configures multiple server groups within a context and applies individual RADIUS server group for subscriber in that context. Each server group consists of a list of AAA servers.

IF no RADIUS group is applied for this subscriber or the default subscriber profile, the default server group available at context level is used for accounting and authentication of the subscriber.

Example

Following command applies a previously configured RADIUS server group named *star1* to a subscriber within the specific context:

```
radius group star1
```

Following command disables the applied RADIUS server group for the specific subscriber.

```
no radius group
```

radius returned-framed-ip-address

Sets the policy whether or not to reject a call when the RADIUS server supplies 255.255.255.255 as the framed IP address and the MS does not supply an address.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

radius returned-framed-ip-address 255.255.255.255-policy { accept-call-when-ms-ip-not-supplied | reject-call-when-ms-ip-not-supplied }

default radius returned-framed-ip-address 255.255.255.255-policy

accept-call-when-ms-ip-not-supplied

Accepts calls when the RADIUS server supplies framed IP address as 255.255.255.255 and the MS does not supply an address.

reject-call-when-ms-ip-not-supplied

Rejects calls when the RADIUS server supplies framed IP address as 255.255.255.255 and the MS does not supply an address.

default

Sets the policy to its default of rejecting calls when the RADIUS server supplies framed IP address as 255.255.255.255 and the MS does not supply an address.

Usage Guidelines

Use this command to set the behavior for the current subscriber when the RADIUS server supplies 255.255.255.255 as the framed IP address and the MS does not supply an address.

Example

The following command sets the subscriber profile to reject calls when the RADIUS server supplies framed IP address as 255.255.255.255 and the MS does not supply an address:

radius returned-framed-ip-address 255.255.255.255-policy reject-call-when-ms-ip-not-supplied

radius rulebase-format

This command enables/disables the Rulebase Concatenation feature at subscriber level. This feature is used to merge the prepaid attribute and SN1-Rulebase as a new rulebase and then apply the new rulebase to the session. If the Rulebase Concatenation feature is not enabled, the last received rulebase is applied to the session.

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

Product

GGSN

PDSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

radius rulebase-format { custom1 | standard }

default radius rulebase-format standard

default

Disables the Rulebase Concatenation feature. The default setting is **standard**.

custom1

Specifies the rulebase as a custom value derived from multiple RADIUS attributes in the RADIUS Access-Accept response message.

standard

Specifies the rulebase as a single attribute value as obtained in RADIUS Access-Accept response message. This is the default setting.

Usage Guidelines

Currently, the Wireless Mobile Private Network (MPN) configures a dedicated rulebase per service. The Enterprise that utilizes this service has the rulebase per subscriber in 3G or signaled from AAA server with SN1-Rulebase attribute. In the case of a prepaid service, the rulebase name will be the customer-specific prepaid policy attribute received from the AAA server.

When both the RADIUS attributes are received, the last received attribute is considered and applied to the subscriber session. This CLI command is used to merge prepaid attribute and SN1-Rulebase as a new rulebase and then apply the new rulebase to the session on the gateway.



Important Rulebase Concatenation is a customer-specific feature and it requires a valid license to enable the feature. For more information, contact your Cisco account representative.

In 18 and earlier releases, rulebase was a single attribute value as obtained in the RADIUS Access-Accept response message. That is, only one rulebase can be applied with either SN1-Rulebase AVP or customer-specific prepaid policy AVP, whichever comes last.

In 19 and later releases, when both the attributes are received, the rulebase name will be a concatenation of the attributes as received in the Access-Accept response message. If only one of the attributes is received, the current behavior is applicable i.e. the last received attribute will be selected as the rulebase and it will be applied to the session.

If the concatenated rulesbase is not matching with the rulebase configured on the gateway, and/or if both the attributes are present more than once, then the session is rejected.

This feature implementation helps the MPN to customize the rulebase and combine prepaid service with additional services like Service Based Access (SBA).

Example

The following command merges the RADIUS attributes and installs the new concatenated rulebase.

```
radius rulebase-format custom1
```

rohc-profile-name

Identifies the robust header compression (RoHC) profile configuration that will be applied to bearer sessions belonging to this subscriber.

Product

HSGW

PDSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

rohc-profile-name *name*

name

Specifies the name of the RoHC profile that the system will use to apply header compression and decompression parameters to bearer session data for this subscriber. *name* must be an existing RoHC profile expressed as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to specify a RoHC configuration profile to be applied to bearer sessions belonging to this subscriber. RoHC profiles are configured through the Global Configuration Mode using the **rohc-profile** command.

Example

The following command specifies that the RoHC profile named *rohc-cfg1* is to be applied to all bearer sessions belonging to this subscriber:

```
rohc-profile-name rohc-cfg1
```

secondary ip pool

Specifies a secondary IP pool to be used as backup pool for Network Address Translation (NAT).

Important This command requires the purchase and installation of a license. Please contact your Cisco sales representative for more information.

Product NAT

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-subscriber)#`

Syntax Description

secondary ip pool *pool_name*

no secondary ip pool

no

Removes the previous secondary IP pool configuration.

secondary ip pool *pool_name*

Specifies the secondary IP pool name.

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

Usage Guidelines Use this command to configure a secondary IP pool for NAT subscribers, which is not overwritten by the RADIUS supplied list. The secondary pool will be appended to the RADIUS supplied IP pool list or subscriber template provided IP pool list, as applicable, during call setup.

Example

The following command configures a secondary IP pool named *test123*:

```
secondary ip pool test123
```

send-destination-pgw

Configures how the HSGW selects a P-GW address for the "Destination-PGW" AVP.

Product HSGW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

send-destination-pgw { all | explicit-only | implicit-only }

no send-destination-pgw

no

Removes the configuration for this command.

all

P-GW address is obtained either by explicit or implicit mechanism.

explicit-only

The UE performs LCP/PPP procedures, and attaches with a specific APN. The HSGW queries the AAA over the STa interface and receives a MIP6-Agent-Info AVP that includes a sub AVP of Destination-Host. The HSGW copies the value of the Destination-Host AVP in the Destination-PGW AVP which is sent in the CCR-I to the PCRF.

implicit-only

The UE performs LCP/PPP procedures, and attaches with a specific APN. The AAA does not return the P-GW to use, so the HSGW performs NAPTR procedures to determine the P-GW which will be used.

Usage Guidelines

Use this command to configure how the HSGW selects a P-GW address for the "Destination-PGW" AVP. This AVP is sent over Gxa to the PCRF.

Example

Configures the HSGW to select either implicit or explicit selection method.

```
send-destination-pgw all
```

service-option

Product

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

[no] service-option *number*

no

Removes the specified service option from the subscriber configuration.

number

Specifies the service option the subscriber is allowed to use. *number* must be a legitimate service option and be an integer value from 0 through 1000.

Usage Guidelines Up to seven service options can be specified for this subscriber.

Example

simultaneous

Enables or disables the simultaneous use of both Mobile and Simple IP services.

Product PDSN

FA

HA

ASN-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description **`[ no ] simultaneous simple-and-mobile-ip`**

no

Disables the simultaneous use.

Usage Guidelines Subscribers with mobile devices that concurrently support mobile and simple IP services require this option to be set.

Example

The following command enables simultaneous use of both Simple and Mobile IP services:

`simultaneous simple-and-mobile-ip`

timeout absolute

Configures the maximum duration of the session before the system automatically terminates the session.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

timeout absolute *seconds*

{ default | no } timeout absolute

default | no

Indicates the timeout specified is to be returned to its default behavior. If a timeout value is not specified, all timeouts are set to their default values.

timeout absolute

Default: 0

Specifies the absolute maximum time a session may exist (in seconds) in any state (active or dormant).

seconds

Specifies the maximum amount of time (in seconds) before the specified timeout action is activated. *seconds* must be an integer from 0 through 4294967295. The special value 0 disables the timeout specified.

Usage Guidelines

Use this command to set the absolute maximum time a session may exist in any state.

Example

The following command configures the absolute maximum timeout to 18000 seconds (300 minutes):

```
timeout absolute 18000
```

timeout idle

Configures the idle timeout duration for the long duration timer associated with a subscriber session.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

timeout idle *idle_dur* **[micro-checkpoint-deemed-idle** *[time_in_seconds]* **| micro-checkpoint-periodicity** *time_in_seconds* **]**

{ default | no } timeout idle

default | no

Indicates the timeout specified is to be returned to its default behavior. If no specific timeout is specified, then all are set to their default behavior.

timeout idle

Default: 0

Specifies the maximum duration of the session (in seconds) can remain idle before the system automatically terminates the session due to inactivity.

idle_dur

Specifies the maximum amount of time (in seconds) before the specified timeout action is activated. *idle_dur* must be an integer from 0 through 2147483647. The special value 0 disables the timeout specified.

micro-checkpoint-deemed-idle *time_in_seconds*

Configures micro-checkpoint duration when UE transitions from Idle to Active and vice versa. *time_in_seconds* must be an integer from 10 through 1000. Default: 180.



Important Micro-checkpoint-deemed-idle value should be less than idle timeout value.

micro-checkpoint-periodicity *time_in_seconds*

Configures periodic idle seconds micro checkpoint timer on a per-subscriber basis. Idle seconds micro checkpoints are sent at the configured regular intervals to the standby chassis; otherwise, they are sent at intervals of 10 seconds, which is the default value.*time_in_seconds* must be an integer value in the range from 10 through 10000.Default: 10.



Important Micro-checkpoint-periodicity value should be less than idle timeout value.

Usage Guidelines

Use this command to set the idle time duration, micro-checkpoint-deemed-idle and micro-checkpoint-periodicity timer for a subscriber session to identify a dormant session.

Important On the fly change from **micro-checkpoint-deemed-idle** to **micro-checkpoint-periodicity**, and vice-versa, is not supported.

Example

The following command sets the idle timeout duration to 60 seconds:

```
timeout idle 60
```

The following command sets the idle timeout duration to 20 seconds and micro-checkpoint-deemed-idle to 15 seconds:

```
timeout idle 20 micro-checkpoint-deemed-idle 15
```

timeout long-duration

Configures the long duration timeout and optionally the inactivity duration of HA subscriber session.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

timeout long-duration *ldt_timeout* **[inactivity-time** *inact_timeout* **]**

[no | default]timeout long-duration

no

Indicates the timeout specified is to be returned to its default behavior. If no specific

timeout is specified then all are set to their default behavior.

long-duration *ldt_timeout*

Default: 0

Designates the maximum duration of the session (in seconds) before the system automatically reports/terminates the session.

ldt_timeout must be a value in the range from 0 through 4294967295. The special value 0 disables the timer.

inactivity-time *inact_timeout*

Specifies the maximum amount of time (in seconds) before the specified session is marked as dormant.

inact_timeout must be a value in the range from 0 through 4294967295. The special value 0 disables the inactivity time specified.

Usage Guidelines

Use this command to set the long duration timeout period and inactivity timer for subscriber sessions. Reduce the idle timeout to free session resources faster for use by new requests.

Refer to the **long-duration-action detection** and **long-duration-action disconnection** commands for more information.

Example

The following command sets the long duration timeout duration to *300* seconds and inactivity timer for subscriber session to *45* seconds:

```
timeout long-duration 300 inactivity-time 45
```

tpo policy

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

tunnel address-policy

Specifies the policy for address allocation and validation for all tunneled calls (IP-IP, IP-GRE) except L2TP calls. With this command enabled, GGSN IP address validation could be disabled for specified incoming calls.

For GGSN systems, this command can also be specified in the APN Configuration mode (**tunnel address-policy**) which would mean the system defers to the old **l3-to-l2-tunnel address policy** command for calls coming through L2TP tunnels.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

tunnel address-policy { alloc-only | alloc-validate | no-alloc-validate }

default tunnel address-policy

alloc-only

Allocates IP addresses locally without validation.

alloc-validate

Default.

The VPN Manager allocates and validates all incoming IP addresses from a static pool of IP addresses.

no-alloc-validate

No IP address assignment or validation is done for calls coming in via L3 tunnels. Incoming static IP addresses are passed. This option allows for the greatest flexibility.

default

Resets the tunnel address-policy to **alloc-validate**.

Usage Guidelines

This command supports scalable solutions for Corporate APN deployment as many corporations handle their own IP address assignments. In some cases this is done to relieve the customer or the mobile operators from the necessity of reconfiguring the range of IP addresses for the IP pools at the GGSN.

Example

The following command resets the IP address validation policy to validate against a static pool of address:

```
default tunnel address-policy
```

The following command disables IP address validation for calls coming through tunnels:

```
tunnel address-policy no-alloc-validate
```

tunnel gre

Configures Generic Routing Encapsulation (GRE) tunnel parameters for the current subscriber.

Product

PDSN

GGSN

ASN-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

tunnel gre peer-address *peer_address* **local-address** *local_addr* **[preference** *num* **]**

no tunnel gre peer-address *peer_address*

peer-address *peer_address*

Specifies the IP address of the external gateway terminating the GRE tunnel.

local-address *local_addr*

Specifies the IP address of the interface in the destination context originating the GRE tunnel.

preference *num*

Default: 1

Assigns a preference to the tunnel.

num can be an integer from 1 through 128.



Important Only one GRE tunnel per subscriber is supported. Therefore, the preference should always be set to "1".

no

Disables GRE tunneling for the current subscriber.

Usage Guidelines Subscriber IP payloads are encapsulated with IP/GRE headers and tunneled by the AGW to an external gateway.

Example

The following command configures the system to encapsulate subscriber traffic using GRE and tunnel it from a local address of *192.168.1.100* to a gateway with an IP address of *192.168.1.225*:

```
tunnel gre peer-address 192.168.1.225 local-address 192.168.1.100
preference 1
```

tunnel ipip

Configures IP-in-IP tunnelling parameters for the current subscriber.

Product PDSN

GGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

tunnel ipip peer-address *peer_address* **local-address** *local_addr* **[preference** *num* **]**

no tunnel ipip

peer-address *peer_address*

Specifies the IP address of the external gateway terminating the IP-in-IP tunnel.

local-address *local_addr*

Specifies the IP address of the interface in the destination context originating the IP-in-IP tunnel.

preference *num*

Default: 1

If multiple tunnels will be configured, this option assigns a preference to the tunnel.

num can be an integer from 1 through 128.

no

Disables IP-in-IP tunneling for the current subscriber.

Usage Guidelines

Subscriber IP payloads are encapsulated with IP-in-IP headers and tunneled by the GGSN or PDSN to an external gateway.

Example

The following command configures the system to encapsulate subscriber traffic using IP-in-IP and tunnel it from a local address of *192.168.1.100* to a gateway with an IP address of *192.168.1.225*:

```
tunnel ipip peer-address 192.168.1.225 local-address 192.168.1.100
preference 1
```

tunnel ipsec

Configures sessions for the current subscriber to use an IPSec tunnel based on the IP pool corresponding to the subscriber's assigned IP address.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

tunnel ipsec use-policy-matching-ip-pooler-address

no tunnel ipsec use-policy-matching-ip-pooler-address

no

Disables the use of the IPSec policy that matches the IP pool that the assigned IP address relates to.

Usage Guidelines

Use this command to set the current subscribers sessions to use an IPSec policy that is assigned to the IP pool that the subscribers assigned IP address relates to.

Example

The following command enables the use of the policy that matches the IP pool address:

tunnel ipsec use-policy-matching-ip-pooler-address

tunnel l2tp

Configures L2TP tunnel parameters for the subscriber.

Product

All products supporting L2TP

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax Description

tunnel l2tp [peer-address *ip address* **[[encrypted] [secret** *secret*]] [**preference** *number*] **[tunnel-context** *context* **] [local-address** *ip_address* **] [crypto-map** *map_name* **{ [encrypted] isakmp-secret** *secret* **}]]**

no tunnel l2tp [peer-address *ip_address* **]**

peer-address *ip_address*

A peer L2TP Network Server (LNS) associated with this LAC (L2TP Access Concentrator). *ip_address* must be an IP address entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal format.

[encrypted] secret *secret*

Specifies the shared key (secret) between the L2TP Network Server (LNS) associated with this LAC (L2TP Access Concentrator). *secret* must be an alphanumeric string of 1 through 63 characters that is case sensitive.

encrypted: Specifies the encrypted shared key between the L2TP Network Server (LNS) associated with this LAC (L2TP Access Concentrator). *secret* must be an alphanumeric string of 1 through 128 characters that is case sensitive.

The **encrypted** keyword is intended only for use by the system 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. Only the encrypted secret is saved as part of the configuration file.

preference *number*

Default: 1

Specifies the order in which a group of tunnels configured for this subscriber will be tried. *number* must be an integer from 1 through 65535.

tunnel-context *context*

Specifies the name of the context containing ports through which this subscriber's data traffic is to be communicated between this LAC and the LNS. *context* must be an alphanumeric string of 1 through 79 characters.

local-address *ip_address*

Specifies a LAC service bind address which is given as a hint that is used to select a particular LAC service. *ip_address* must be an IP address entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

crypto-map *map_name* { [encrypted] isakmp-secret *secret* }

Specifies the name of a crypto map that has been configured in the current context. *map_name* must be an alphanumeric string from 1 to 127 alphanumeric characters.

isakmp-secret *secret*: Specifies the pre-shared key for the Internet Key Exchange (IKE). *secret* must be an alphanumeric string of 1 through 127 characters.

encrypted isakmp-secret *secret*: Specifies the pre-shared key for IKE. Encryption must be used when sending the key. *secret* must be an alphanumeric string of 1 through 127 characters.

no

Disables tunneling for the current subscriber. When peer-address is included, the tunneling for that specific L2TP Network Server (LNS) is disabled but tunneling to other configured LNSs is still enabled.

Usage Guidelines

Use this command to configure specific L2TP tunneling parameters for the current subscriber.

Example

To specify L2tp tunneling to the LNS peer at the IP address *198.162.10.100* with a shared secret of *bigco* and preference of *1*, enter the following command:

```
tunnel l2tp peer-address 198.162.10.100 secret bigco preference 1
```

w-apn

This command allows you to configure the default APN to be used for the UE connections when the AAA server does not return the subscriber APN name in the service-selection AVP in RADIUS Access-Accept message.

Product

eWAG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax Description

w-apn *apn_name*

no w-apn

no

If previously configured, removes the specified configuration.

apn-name *apn_name*

Specifies the APN name.

apn_name must be the name of an APN and must be a string of 1 to 62 characters in length consisting of alphabetic characters (A-Z and a-z), digits (0-9), dot(.) and the dash (-).

Usage Guidelines

Use this command to configure the default APN to be used for UE connections when the AAA server does not return the subscriber APN name in the Service-Selection AVP in RADIUS Access-Accept message. This APN will be considered as the network to which the UE is connecting and used in the CPC request message towards GGSN.

Example

The following command configures an APN named *apn123*:

w-apn apn123